

UNITED STATES DISTRICT COURT

for the
Southern District of Texas

United States Courts Southern
District of Texas
FILED

May 8, 2023

Nathan Ochsner, Clerk of Court

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Case No. **4:23-mj-981**

iPhone Associated with Phone Number 941-456-3635 and IMEI
356172090590826, Currently in the Evidence Vault, as Non-drug
Exhibit 85, in the Custody of the Drug Enforcement Administration

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

iPhone Associated with Phone Number 941-456-3635 and IMEI 356172090590826, Currently in the Evidence Vault, as Non-drug Exhibit 85, in the Custody of the Drug Enforcement Administration, located in the Southern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachments A and B to the Affidavit in Support of an Application for Search Warrant.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841(a)(1)	Unlawful distribution of controlled substances
21 U.S.C. § 846	Conspiracy to unlawfully distribute controlled substances
21 U.S.C. § 856(a)(1)	Maintaining a drug-involved premises

The application is based on these facts:

See attached affidavit in support of search warrant application.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Cesar Hernandez
Applicant's signature

Cesar Hernandez, DEA Task Force Officer
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone _____ (specify reliable electronic means).

Date: 05/08/2023

Christina A. Bryan
Judge's signature

City and state: Houston, Texas

Hon. Christina A. Bryan, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN THE MATTER OF THE SEARCH OF:
iPhone Associated with Phone Number 941-
456-3635 and IMEI 356172090590826,
Currently in the Evidence Vault, as Non-drug
Exhibit 85, in the Custody of the Drug
Enforcement Administration

Case No. **4:23-mj-981**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT

I, Melvinla Morgan, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant to search the iPhone associated with phone number 941-456-3635 and IMEI 356-172-090-590-826, belonging to Jonathan Rosenfield, M.D. (“ROSENFELD”), as described in Attachment A, currently in the custody of the Drug Enforcement Administration (“DEA”) located at 1433 West Loop South, Houston, Texas 77027 (“SUBJECT DEVICE”). The applied-for warrant would authorize the forensic examination and review of the SUBJECT DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.
2. On August 20, 2019, a grand jury sitting in the Southern District of Texas returned a twelve-count indictment charging Jonathan Rosenfield, M.D. (“ROSENFELD”); Elmer Taylor; Alantha Stewart Taylor; Kwana Broussard; Ricky Wayne Moten; Sokari Manuel Bobmanuel, R.Ph.; Ardella Fisher, F.N.P.; Enna Amedome, F.N.P.; Otukayode Adeleke Otufale; Jasmine Maynes; Jabrai Price; and Shawneece Deyampert (“the Defendants”) with violations of the Controlled Substances Act (“CSA”) arising out of

- the defendants' roles as medical professionals, owners, pharmacy employees, and "crew leaders" at medical clinics and a pharmacy that allegedly distributed and dispensed controlled substances—oxycodone and hydrocodone—with no legitimate medical purpose and outside the usual scope of professional practice.
3. On April 26, 2023, a grand jury sitting in the Southern District of Texas returned a Superseding Indictment against the remaining four defendants, ROSENFELD, Bobmanuel, Amedome, and Deyampert, who are set for trial before the Honorable Randy Crane on June 5, 2023. The other eight defendants have pleaded guilty to conspiracy to distribute and dispense controlled substances, in violation of 21 U.S.C. § 846.
 4. On August 27, 2019, the Honorable Peter Bray authorized the search and seizure of the SUBJECT DEVICE, associated with phone number 941-456-3635 ("Original Warrant"), which is attached as Exhibit A. The Original Warrant was obtained in the Southern District of Texas although the SUBJECT DEVICE was located in the Northern District of Georgia. On August 28, 2019, ROSENFELD was arrested in Atlanta, Georgia by members of the United States Marshal Service ("USMS") and the Drug Enforcement Administration's ("DEA") Atlanta Tactical Diversion Squad. The affiant on the Original Warrant was aware that ROSENFELD was not located in Houston at the time the Original Warrant was sworn out but did not appreciate that the Original Warrant could not be executed on the SUBJECT DEVICE if it was located outside of the Southern District of Texas. The affiant on the Original Warrant was not part of the team that executed the arrest of ROSENFELD and the seizure of the

SUBJECT DEVICE. The affiant on the Original Warrant, a TFO with DEA, has since returned to his home agency, the Department of Public Safety.

5. According to the DEA report on ROSENFELD's arrest, a DEA Task Force Officer ("TFO") removed two cell phones from ROSENFELD's immediate area in the master bedroom, one of which was identified as the SUBJECT DEVICE and was seized pursuant to the Original Warrant. The arresting officers were not members of the investigative team, but rather local DEA and USMS agents assisting on the arrest in Georgia. Had the SUBJECT DEVICE not been seized pursuant to the Original Warrant, the arresting officers could have seized the SUBJECT DEVICE because it was seized incident to arrest, and it was in plain view and known to contain evidence of the criminal activity alleged in the Indictment. Further, after ROSENFELD was taken into custody, but before the phone was unlocked, agents observed that ROSENFELD's phone continued to receive text messages.
6. Because ROSENFELD refused to unlock the SUBJECT DEVICE using either his thumb, his face, or a password, DEA TFOs, in an effort to preserve the ability to access the SUBJECT DEVICE in the future (and knowing from training and experience that by unlocking a cell phone, agents can place the phone in airplane mode to ensure that the evidence on the phone cannot be remotely deleted), agents obtained the assistance of a Special Agent with the Georgia Department of Revenue to obtain and access data from the SUBJECT DEVICE. That process took approximately one month. On September 25, 2019 Georgia DEA TFOs mailed the SUBJECT DEVICE, along with the digital hard drive containing its contents, to DEA Houston.

7. Since that time, members of the prosecution team have reviewed the contents of the SUBJECT DEVICE, which was redacted for potentially privileged material. I have not personally reviewed the contents of the SUBJECT DEVICE, nor has the Applicant, TFO Cesar Hernandez. A copy of the (unredacted) SUBJECT DEVICE was produced to the Defendants in discovery on January 28, 2021. On November 1, 2021, a report pertaining to the search of the SUBJECT DEVICE was produced to the defendants in discovery, and on April 10, 2023, the affidavit in support of the Original Warrant was produced to the defendants in discovery.
8. Based on the probable cause included in this affidavit, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the government to utilize the image obtained in August 2019 pursuant to the Original Warrant, as there is no reason to believe that image is any different from an image that would be obtained anew. Further, the image obtained pursuant to the Original Warrant in August 2019 went through a filter process to remove potentially privileged information from the prosecution team's possession, and was produced to all defendants in January 2021. In the alternative, the warrant I am applying for would permit the examination of the SUBJECT DEVICE consistent with the warrant anew. This examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

IDENTITY AND EXPERIENCE OF AFFIANT

9. I am presently employed as a Diversion Investigator ("DI") with the DEA and have been so employed for approximately eight years. Prior to my employment with DEA,

I was a program specialist with the Department of State Health Services for the State of Texas, for three years. I received my Bachelor of Science Degree in sociology from Lamar University located in Beaumont, Texas, and I received my Master's Degree in Behavioral Sciences from the University of Houston at Clear Lake.

10. As a DI, I conduct regulatory, civil, and criminal investigations of DEA registrants related to their controlled substances activities. During my career as a DI, I have participated in a number of investigations of DEA registrants (individuals/entities that maintain DEA Registration Numbers) related to their improper prescribing, dispensing, and distributing of controlled substances. During my thirteen-week Basic DI Training in Quantico, Virginia, I received the training necessary to conduct these types of investigations. I am knowledgeable of the laws, regulations, and procedures pertinent to investigations of the diversion of controlled substances to the illicit market as well as the techniques employed by registrants to divert controlled substances, that is, the illegal dispensing or distribution of controlled substances for other than legitimate purposes.

11. Through my experience as a DI in Houston, I have become familiar with how drug trafficking organizations ("DTOs") operate pharmacies as fronts for the illegal distribution of Schedule II opioids including hydrocodone and oxycodone, and of other controlled substances, such as carisoprodol, alprazolam, and promethazine syrup with codeine. In addition to what I have learned from personal observation during my own investigations about the methods and practices of individuals trafficking in or diverting pharmaceutical drugs, I have gained knowledge about these matters from conversations with pharmacists; physicians; other DEA investigators, agents, and TFOs; other law

enforcement agents and investigators; state medical board investigators; pharmacy board investigators; and others.

12. I have also conducted and participated in debriefing many individuals involved in diverting controlled substances, through which I have learned valuable information regarding the techniques used by pharmaceutical drug wholesalers and DTOs to illegally distribute controlled substances. In addition, I am familiar with the instrumentalities pharmaceutical drug traffickers use to conduct their illegal business, including instant messaging and email services; electronic devices, including cellular telephones and computers; and vehicles.¹

PURPOSE OF THE AFFIDAVIT

13. Based on my training, experience, and the facts set forth in this Affidavit, I have probable cause to believe the Defendants, and others known and unknown, have committed violations of the CSA, including: 21 U.S.C. § 841 (Distribution of Controlled Substances); 21 U.S.C. § 846 (Conspiracy to Distribute Controlled Substances), 21 U.S.C. § 856(a)(2) (Maintaining a Drug-Involved Premises) (“SUBJECT OFFENSES”). I also have probable cause to believe that SUBJECT DEVICE, more particularly described below and as set forth in Attachment A, contains

¹ As a Diversion Investigator with DEA, I can be the affiant, but not the *applicant*, for the warrants requested. For that reason, for the purpose of the warrant requested, DEA TFO Cesar Hernandez from the Conroe Police Department (“Conroe PD”), currently sworn as a Federal Task Force Officer with the DEA, will be the applicant. TFO Hernandez is a “federal law enforcement officer” under Fed. R. Crim. P. 41(a)(2)(C), and he is within a category of officers authorized by the Attorney General to request a search warrant. TFO Hernandez was a patrol officer for three years at Conroe PD, and was previously a patrol officer with Montgomery County Sheriff’s Office for two years before that. TFO Hernandez has worked in partnership with narcotics officers, interacted with drug users and drug traffickers, and has training and experience recognizing the behaviors associated with drug trafficking. TFO Hernandez has also completed in-service training that covered drug trafficking investigations. He has experience seeing the use of telecommunications devices, including cell phones, in drug-related criminal investigations. Further, he is familiar with suspects’ use of evasive language to avoid detection of criminal activity by law enforcement.

evidence, instrumentalities, and fruits of these crimes, more particularly described in Attachment B.

14. The information in this affidavit is derived from my participation in this investigation and information obtained from several sources, including: Oral and written reports about this and other investigations, which I received from various federal and local law enforcement agencies; physical surveillance and undercover operations conducted by investigators that were directly or indirectly reported to me; telephone toll records, public sources, and business records; information from a medical doctor who is an expert in the field of pain management; and information from Confidential Informants (CI#2,² CI#3, CI#4³), which was only relied upon once it had been deemed reliable through independent corroboration of information provided.⁴ Further, much of the same information from the Original Warrant is included in the section on probable cause, all of which was information known to the investigation prior to the execution of the Original Warrant in August 2019.

15. Because this affidavit is submitted for the limited purpose of securing authorization for a search and seizure warrant, I have not included each and every fact known to me

² CI#2 was a cooperating defendant who, at the time of his/her cooperation, was seeking credit for his/her cooperation. At the time of CI#2's sentencing, which occurred after his/her cooperation in this case, the government moved for a downward departure under the Sentencing Guidelines. Operations involving CI#1 were included in the original affidavit. Since that time—and after his/her participation in this investigation—CI#1 has been found to be uncooperative, unrelated to their role in this investigation. Accordingly, the information relating to CI#1 is not included in the current affidavit.

³ CI#3 and CI#4 are confidential informants paid by the DEA. Following CI#3's assistance in this case, CI#3 was deactivated as a confidential informant. CI#3 was recently imprisoned following an aggravated robbery, which was unrelated to his/her assistance in this case.

⁴ While not all information provided by CIs could be independently corroborated, sufficient information from the CIs was corroborated and could be relied upon. Based on my training, experience, and knowledge of the facts of the investigation, I believe that the CIs used in this case at the time were/are reliable.

concerning this investigation. I have set forth only the facts that I believe are essential to establish the necessary foundation for the requested search warrant.

BACKGROUND

I. Relevant Statutes and Regulations

16. 21 U.S.C. § 841(a)(1) makes it unlawful for any person to knowingly and intentionally distribute or dispense a controlled substance except as authorized by law. A medical professional violates this statute by knowingly and intentionally distributing or dispensing a controlled substance for no legitimate medical purpose and not in the usual course of professional medical practice. *United States v. Rosen*, 582 F.2d 1032, 1034 (5th Cir. 1978).

17. 21 U.S.C. § 846 prohibits an agreement between two or more persons to unlawfully distribute or dispense controlled substances.

18. 21 U.S.C. § 856(a)(1) makes it unlawful to “knowingly open, lease, rent, use, or maintain any place, whether permanently or temporarily, for the purpose of manufacturing, distributing, or using any controlled substance.”

19. According to 21 C.F.R. § 1306.14, every person who dispenses a controlled substance must be registered to do so with the DEA. 21 C.F.R. § 1306.04(a) further provides:

A prescription for a controlled substance to be effective must be issued for a legitimate medical purpose by an individual practitioner acting in the usual course of his professional practice. The responsibility for the proper prescribing and dispensing of controlled substances is upon the prescribing practitioner

20. Both federal and state law provide for the maintenance of medical records and inventory. 21 C.F.R. § 1304.04 requires registrants to keep, and to make available to the DEA for inspection and copying, medical records and inventory for at least two years from the inventory or record date. In addition, 22 Texas Administrative Code §

- 165.1 requires physicians licensed by the Texas Medical Board (“TMB”) to maintain complete, contemporaneous, and legible patient records that document each patient encounter with respect to (1) the “reason for the encounter and relevant history, physical examination findings, and prior diagnostic test results;” (2) an “assessment, clinical impression, or diagnosis;” (3) a “plan of care,” including, if appropriate, a plan for discharge; and (4) the “date and legible identity of the observer.”
21. 21 U.S.C. § 822 states that, aside from some exceptions not relevant here, controlled substances may only be prescribed, dispensed, or distributed by persons registered with the DEA. *See also* 21 C.F.R. § 1306.04.
22. The Prescription Monitoring Program (“PMP”) is a database of all reported prescriptions for controlled substances that are issued and dispensed in Texas.
23. Both federal and state law provide for the maintenance of pharmacy records and inventory. *See, e.g.*, 21 C.F.R. § 1304.04 (records must be maintained at least two years from the inventory or record date); 22 Texas Admin. Code § 291.34(a)(1)(A) (establishing same requirement of Texas pharmacies).

II. Relevant Controlled Substances

24. 21 U.S.C. § 812 establishes five schedules of controlled substances—Schedules I, II, III, IV, and V—based on the drug’s potential for abuse, its currently accepted medical use, and the severity of physical or psychological dependence that could result from its abuse. Pharmaceutical controlled substances are listed in Schedules II through V because they are considered drugs for which there is an accepted medical use, but which pose a substantial potential for abuse and addiction. Relevant here,

a. **Oxycodone** is the generic name for a Schedule II analgesic drug that is typically prescribed for moderate-to-severe pain relief. Due to its potential for addiction,

oxycodone prescriptions are generally issued for a modest number of pills to be taken over a short period of time. Oxycodone is a commonly abused and diverted controlled substance.

b. **Hydrocodone** is the generic name for a narcotic analgesic that was reclassified from a Schedule III to a Schedule II controlled substance as of October 6, 2014. Hydrocodone is sold under several brand names, including Norco. Hydrocodone is a commonly abused and diverted controlled substance.

c. **Carisoprodol** is a Schedule IV controlled substance. It is classified as a muscle relaxant. According to the Food and Drug Administration (“FDA”), carisoprodol should only be used for acute treatment periods of up to two to three weeks. According to recent expert testimony in a similar case, I know that carisoprodol is “a drug of abuse without any proof of efficacy.” Additionally, when taken with oxycodone or hydrocodone, carisoprodol can cause an increased sensation of euphoria, which increases its potential for abuse and risk of death.

III. The illegal process of diverting prescription drugs

25. Based upon my training and experience, illegal pain management clinics and pharmacies that operate as “pill mills” are generally comprised of owners and operators; physicians, pharmacists, and other medical providers; and office staff.

26. A “crew leader” is usually someone who finds and pays individuals, some of whom are homeless or impoverished, to pose as chronic pain patients; transports them (often in groups) to the clinic; coach the patients to fill out patient intake documentation to support a prescription for pain medication and pays for the “visit with the doctor” (i.e., the illegitimate prescription); takes the patient (or just the illegitimate prescription) to the pharmacy; and pays for and takes control of the prescription drugs, often to divert and sell them on the street for profit.

27. Often, the clinic and pharmacy owners/operators coordinate with the crew leaders to set aside appointments for individuals the crew leaders bring to the clinic. The clinic often charges a flat fee, paid up front—before the patient sees the physician—usually in cash, based on the controlled substance the physician will later prescribe. For example, a patient might pay \$300 at the beginning of a visit knowing the resulting

- prescription will be for hydrocodone, or \$500 at the beginning of a visit, knowing the resulting prescription will be for oxycodone.
28. The actual doctor visit—if any—usually includes only a perfunctory consultation. At the conclusion of the visit, the physician almost always orders a Schedule II opioid, such as hydrocodone or oxycodone, and routinely a second for a Schedule IV drug such as alprazolam (a drug used to treat anxiety) or carisoprodol. These prescriptions are issued without a legitimate medical purpose and outside the scope of professional practice.
29. Some pharmacies require each “patient” to present his/her own prescription; others allow crew leaders to present the patients’ IDs for copying. The crew leaders (whether directly or through their “patients”) usually pay in cash, even if they have insurance, which allows the pharmacy to charge above-market rates without leaving a paper trail for insurance providers, including private insurance, Medicare, and Medicaid; and by DEA and other law enforcement. For example, according to pharmacists with knowledge of market rates, around August 2019, legitimate pharmacies may have charged \$42.00 for 120 dosage units of oxycodone 30mg and \$6.00 for 90 dosage units of carisoprodol 350mg, while pill-mill pharmacies may have charged as much as \$1,340 for that combination. These prices reflect the high market value of the drugs on the illegal drug market.
30. Based on my training and experience, I know that “pill mill” clinics and pharmacies often attempt to avoid detection by law enforcement by: falsifying patient records and prescriptions, accepting a combination of pain management and family medicine patients, requiring appointments, requiring patients to have prior prescriptions for

controlled substances on the PMP, papering patient files with x-ray or MRI results that are rarely reviewed or verified, maintaining irregular business hours, depositing only a portion of the cash proceeds in the bank.

PROBABLE CAUSE OF VIOLATIONS OF LAW

31. On August 20, 2019, a grand jury sitting in the Southern District of Texas returned an indictment charging the Defendants with violations of the CSA. ROSENFELD is charged with conspiracy to distribute and dispense controlled substances without a legitimate medical purpose, outside the usual course of professional practice, in violation of 21 U.S.C. § 846; unlawful distribution of a controlled substance, in violation of 21 U.S.C. § 841; and maintaining a drug-involved premises, in violation of 21 U.S.C. § 856. On April 26, 2023, a grand jury in the Southern District of Texas returned a Superseding Indictment, in which ROSENFELD is charged with the same violations of the CSA.

32. Based on the evidence described further below, there is probable cause exists to believe that the SUBJECT DEVICE contains evidence, fruits, and instrumentalities of the SUBJECT OFFENSES.

I. Relevant Individuals and Entities

33. Elmer Taylor and Alantha Stewart, husband and wife, owned and operated two clinics that operated as pill mills, both called SunnySide Wellness. Sunnyside had two locations in the Houston area: one on Edfield Street (“Sunnyside #1”) and on Pinemont Drive (“Sunnyside #2”), collectively (“Sunnyside”). Stewart formed Sunnyside Wellness Center, LLC on May 17, 2018, and was listed as its Manager. Taylor recruited patient-runners and purported patients to buy controlled substances not for a legitimate medical purpose and outside the usual course of professional practice. On

January 6, 2020, and February 3, 2020, Stewart and Taylor, respectively, pleaded guilty to conspiracy to distribute and dispense controlled substances without a legitimate medical purpose and outside the usual course of professional practice for their roles at Sunnyside.

34. ROSENFELD, a resident of Atlanta, Georgia, is a Medical Doctor, and was licensed to practice medicine in the State of Texas beginning in or around December 2017, including during the course of the conspiracy between in or around May 2018 and in or around August 2019. At the time of indictment in August 2019, ROSENFELD maintained a DEA Registration Number, which allowed him to prescribe Schedule II through V controlled substances. ROSENFELD was the purported owner of SunnySide Medical, PLLC, which he formed as a Professional Limited Liability Company in or around October 2018. SunnySide Medical, PLLC, used the assumed name “SunnySide Wellness.” ROSENFELD was the prescribing physician at Sunnyside #1 and its owner on paper, and was the Medical Director at Sunnyside #2. According to PMP records and the investigation, ROSENFELD prescribed large volumes of controlled substances—primarily oxycodone 30mg, hydrocodone 10/325mg, and carisoprodol 350mg—out of Sunnyside without a legitimate medical purpose and outside the usual course of professional conduct.

35. Paul Kobza is a Doctor of Osteopathic Medicine, and was licensed to practice in the State of Texas beginning in or around August 2002. Kobza was purportedly the physician at Sunnyside #2, and, according to PMP and the investigation, he prescribed large volumes of controlled substances—primarily oxycodone 30mg, and hydrocodone

10/325mg—out of Sunnyside #2 without a legitimate medical purpose and outside the usual course of professional conduct.

36. Ardella Fisher was a Family Nurse Practitioner (“NP”) licensed to practice in the State of Texas since beginning in or around November 2017. According to the TMB, ROSENFELD was Fisher’s supervising physician. Fisher worked at Sunnyside #1. On March 10, 2020, Fisher pleaded guilty to conspiracy to distribute and dispense controlled substances without a legitimate medical purpose and outside the usual course of professional practice for her role at Sunnyside. Enna Amedome was also an NP licensed to practice in the States of Texas beginning in or around September 2017.⁵ Amedome worked at Sunnyside #2. According to TMB, Kobza was Amedome’s supervising physician. As NPs, Fisher and Amedome had the authority to prescribe Schedule III through V controlled substances—but not Schedule II’s like oxycodone and hydrocodone—if those prescriptions were issued for a legitimate medical purpose in the usual course of business. Amedome remains pending trial on June 5, 2023.

II. Evidence of Red Flags Observed at Sunnyside

37. During the course of the investigation, CIs visited Sunnyside #1 and #2. Through their in-person visits, footage obtained through video surveillance directed at both Sunnyside #1 and #2, surveillance, photos, PMP data, and other investigative tools, agents learned that Sunnyside operated as a pill mill. The following “red flags” were observed at Sunnyside #1 and #2 during the course of the investigation:

a. Individuals—posing as patients—were often brought to Sunnyside in groups by “crew leaders.” These crew leaders often sat in their cars in the parking lot until their patients were ready to be brought into the clinic. Surveillance showed many of the

⁵ The original warrant mistakenly stated that Amedome was licensed as a NP in the State of Texas since in or around *November* 2017. The Board of Nursing website confirms she was licensed beginning in or around *September* 2017.

same vehicles parked in Sunnyside parking lots on several occasions. Several CIs familiar with pill mills visited Sunnyside and observed known crew leaders bring individuals posing as patients to Sunnyside.

b. Sunnyside #1 and #2 did not accept insurance; it was an all-cash business. Sunnyside charged \$200 to \$300 for hydrocodone and carisoprodol and between \$400 and \$500 for oxycodone and carisoprodol. Individuals seeking prescriptions paid cash *before* seeing the physician based on the prescription they would later receive from ROSENFELD or Kobza.

c. Sunnyside #1 and #2 employed several armed security guards in the parking lot and inside the clinic. These guards controlled patient flow and helped enforce Sunnyside's rules.

d. The majority of individuals who visited Sunnyside posing as patients were prescribed the same or similar combinations of controlled substances with the same or similar dosage units (number of pills), notwithstanding the patients' varied characteristics (age, weight, sex, medical history, diagnosis, etc.). Most often, the patients were prescribed the highest strength pills of short-acting oxycodone, hydrocodone, and carisoprodol available on the market.

III. Cooperating Individuals

38. **CI#2:** On or about February 2, 2019, CI#2 met with Taylor, Stewart, and Fisher at a restaurant in Houston to discuss CI#2 working at Sunnyside #2 as a medical professional. At the meeting Taylor told CI#2 that the clinic had made "a million dollars" in the past nine months at the clinic. Taylor also told CI#2 that Fisher wrote prescriptions for Soma (carisoprodol) and that ROSENFELD gave Stewart the access code to ROSENFELD's electronic prescribing so that Stewart could prescribe under ROSENFELD's name from her cell phone. Taylor told CI#2 that sometimes they used Pharmacy A to fill some of their prescriptions, and that Pharmacy A does not report everything they dispense to the pharmacy board.

39. On March 22, 2019, CI#2 recorded another meeting with Taylor, Stewart, and Fisher at Sunnyside #1 to discuss CI#2 working at Sunnyside #2. During the meeting, Taylor told CI#2 that, "We 100% certified with the state...so your license will be protected."

Taylor told CI#2 that Sunnyside Wellness was “franchised” and that 5400 Pinemont (Sunnyside #2) would also be called Sunnyside Wellness, and would be ready to go soon. CI#2 also inquired about prescribing electronically (“e-prescribe”). Taylor responded that the process was easy and that CI#2 would be sent a “hard token” that would be set up on CI#2’s phone, or a key card, to make sure CI#2 is “pushing” the e-prescriptions through. Stewart also spoke with CI#2 about delegating responsibilities to nurse practitioners. Taylor told CI#2 that CI#2 would hire a nurse and “you make money through her...she can e-scribe for you.”

40. Based on my training and experience, and my participation on this case, I know that when Taylor referenced that Sunnyside #2 was “certified with the state,” he was referring to its status as a registered pain clinic, which is required if a clinic prescribes more than 50% pain medication. But simply registering as a pain clinic does not allow physicians or clinics license to prescribe outside the scope of professional practice or without a legitimate medical purpose. According to the TMB, a pain management certification is location specific and is not transferable to other locations. Based on this information, Sunnyside #1 was a registered certified pain management clinic since February 2019 and Sunnyside #2 is not a registered certified pain management clinic. I also know that in the State of Texas, nurse practitioners are not allowed to e-scribe Schedule II drugs for a physician, nor is a nurse practitioner allowed to prescribe Schedule II drugs for a physician even after an in-person patient visit.

41. **CI#3:** CI#3 told agents that on May 16, 2019, *before* CI#3 became a confidential source, he/she was paid \$70 by a runner to go to Sunnyside #1 to obtain a prescription for hydrocodone. CI#3 said that he/she was seen by Fisher. CI#3 told agents that he/she

told the nurse that he/she had lower back pain. CI#3 described to agents that during the patient visit, Fisher only asked for him/her to breathe in and out and did not perform a physical examination. CI#3 told agents that CI#3 gave a copy of his/her ID to a runner to fill the prescriptions, and that CI#3 did not fill or receive the prescriptions himself/herself. PMP data corroborates that on May 16, 2019, a pharmacy filled 110 dosage units of hydrocodone 10/325mg purportedly issued to CI#3 by ROSENFELD (although CI#3 never saw ROSENFELD). Based upon my training and experience I know that Fisher's purported "treatment" of CI#3 was outside the course of professional practice. Additionally, as a NP, Fisher cannot prescribe Schedule II controlled substances.

42. On or about June 26, 2019, after CI#3 had become a DEA CI, CI#3 made a consensually recorded visit to Sunnyside #2 to obtain prescriptions for controlled substances. CI#3 stated when he/she entered the clinic there were not a lot of people in the front waiting area. CI#3 stated he/she talked with an unidentified black male that who was sitting in the front waiting area and told CI#3 that earlier in the day there were a lot of people. CI#3 stated the unidentified black male told him/her that he goes to the doctor for someone and that he is paid \$100.

43. CI#3 stated that while inside the clinic, another unidentified black male introduced himself as "Nayda" and told CI#3 that he was a recruiter and that he pays \$100 for people to go to the doctor.

44. CI#3 stated when he/she was called to the back that he/she had to give a urine sample and later he/she gave the urinalysis sample to a black female office employee named Ruth LNU. CI#3 stated Ruth did not take his/her blood pressure and that he/she paid

\$460 cash for the visit to Ruth. CI#3 stated Ruth told him/her that \$60 was for physical therapy.

45. CI#3 said that he/she was later seen by Amedome. CI#3 stated he/she told the clinic he/she had lower back pain. CI#3 described to agents that Amedome only asked for him/her to breathe in and out and did not perform a physical examination.

46. CI#3 stated he/she observed two armed security guards at the clinic. CI#3 stated in the back waiting area, he/she observed security cameras on the inside/outside of the clinic almost set up like “the one on Cullen,” which is the location of Sunnyside #1.

47. CS#3 stated after his/her visit with Amedome he/she was told that he/she had to do physical therapy. CI#3 stated while he/she was waiting for physical therapy, he/she observed another unidentified black male tell about 4-5 people (or more) who were waiting on physical therapy, “come on we don’t need it.” CI#3 stated the people got up and left with the unidentified black male. CI#3 stated shortly thereafter he/she got up and departed as well.

48. Audio of CI#3’s visit shows that the physical exam lasted approximately 21 seconds, and the full visit with Amedome lasted approximately 2 minutes. Based upon my training and experience, I have probable cause to believe that Amedome’s purported “treatment” of CI#3 fell outside the usual course of professional practice. On or about July 5, 2019, agents had CI#3 fill the prescription issued by Kobza (although CI#3 never saw Kobza) to CI#3 for 115 pills of oxycodone 30mg at a local pharmacy for \$1,000. Again, nurse practitioners like Amedome are not allowed to prescribe Schedule II controlled substances in the State of Texas.

49. CI#4: On or about June 26, 2019, CI#4 made a consensually recorded visit to Sunnyside #2 to obtain prescriptions for controlled substances. CI#4 stated when/she entered the clinic he/she sat in the front waiting area. CI#4 stated when he/she was called to the back that he/she went into an exam room where two black females entered the room. CI#4 later identified one of the black females, as Deija Wright, a Sunnyside #2 employee. CI#4 stated his/her blood pressure and weight was taken. CI#4 stated he/she was asked some medical history questions.

50. CI#4 stated he/she was asked “What is your pain level 1 through 10?” CI#4 stated “twelve” jokingly. CI#4 was told “A ten, that’s really what you wanna say . . .”⁶ CI#4 was then asked “Who you here with are you here with someone today?” CI#4 stated, “No, I’m here by myself.” CI#4 was asked, “You here by yourself really or did someone bring you here?” CI#4 stated, “By myself.” Deija Wright stated, “You have to pay me for your visit today?” CI#4 stated, “Yes,” Deija Wright asked, “What you gettin?” CI#4 stated, “Norco and Soma.” Deija Wright stated “Norcos is \$300.” CI#4 later paid Deija Wright \$300. I know from my training and experience that it is outside of the usual course of professional practice for a clinic to ask a patient “what you getting” before they are examined by a doctor—especially when considering they are prescribing highly addictive controlled substances.

51. After CI#4 paid the money, he/she sat in the back waiting area where he/she could see the security camera screens on a big television. CI#4 also observed a black male armed security guard. CI#4 stated later, Deija Wright approached him/her with a computer

⁶ The Original Warrant stated that CI#4 was told, “A ten, that’s pretty much want to say a 10.” Because this statement appeared to miss a word, a re-review of the recording sounded as though the statement above was made in response.

- asking for his/her signature. CI#4 stated, “No” jokingly. Deija Wright stated “it’s just consent stating that you cannot sell or trade any medication that you are prescribed.” CI#4 asked “Why?” Deija Wright stated “Cause you can’t.”
52. CI#4 said later he/she was seen by a black female. CI#4 later identified the black female as NP Amedome. CI#4 stated he/she told the clinic he/she had lower back pain. CI#4 described to agents that Amedome only asked for him/her to breathe in and out, squeeze her finger which lasted approximately 35 seconds. Amedome did not perform a physical examination. The entire encounter with Amedome lasted approximately 2 minutes and 10 seconds. As CI#4 exited he/she observed about 10-12 people sitting in the front waiting area.
53. A review of the video shows that the physical exam lasted approximately 32 seconds, and the full visit with Amedome lasted approximately 2 minutes and 15 seconds. Based upon my training and experience, I know that Amedome’s purported “treatment” of CI#4 fell outside the usual course of professional practice.
54. Sunnyside #2 sent CI#4’s prescription to CORNERSTONE Rx PHARMACY, INC. (the owner of which is one of the Defendants pending trial), to fill the prescription, and CI#4 received 114 pills of hydrocodone 10-325mg issued by Kobza, although CI#4 never saw Kobza.⁷ (The prescription bottle indicated CI#4 received 115 hydrocodone 10-325mg pills.) CI#4 also received two prescriptions issued by Amedome for non-controlled substances.

⁷ The Original Warrant mistakenly stated that CI#4 received a prescription for oxycodone 30mg, not hydrocodone 10-325mg. The correct drug is hydrocodone 10-325mg.

IV. PMP Data

55. ROSENFELD's and Kobza's prescription patterns support probable cause to believe that their prescriptions were largely issued outside the usual course of professional practice and with no legitimate medical purpose. The investigation showed that most of the prescriptions ROSENFELD and Kobza issued were e-prescribed.

56. According to the PMP, from in or around May 2018 through on or about August 12, 2019, ROSENFELD issued prescriptions for almost 1.8 million controlled substance pills—approximately 739,000 of those pills were oxycodone. Almost all of these were for oxycodone 30mg—the most potent short-acting oxycodone pill available on the market. Over 90% of all of the pills ROSENFELD prescribed were for either oxycodone, hydrocodone, or carisoprodol, and many of the prescriptions were dangerously combined with each other. Almost all of the prescriptions for these three drugs were for the highest strengths available on the market.

DRUG NAME	PILLS	% OF TOTAL
Oxycodone 30mg	739,377	41%
Carisoprodol 350mg	495,786	28%
Hydrocodone 10/325mg	398,592	22%
TOTAL	1,896,266	91%

57. From on or about April 8, 2019 through on or about August 12, 2019, while Kobza was the supervising physician of Sunnyside #2, Kobza issued prescriptions for a total of 352,193 pills of oxycodone 30mg. The data shows that 82% of Kobza's controlled substance prescriptions were for the oxycodone 30mg. Similar to ROSENFELD, Kobza almost always prescribed the highest available dosages of oxycodone (30mg) and hydrocodone (10/325mg).

DRUG NAME	PILLS	% OF TOTAL
Oxycodone 30mg	352,193	82%
Hydrocodone 10/325mg	51,822	12%
TOTAL	404,015	94%

**PROBABLE CAUSE TO BELIEVE THAT EVIDENCE OF CRIMES IS LOCATED ON
THE SUBJECT DEVICE**

58. Based on evidence derived from the investigation and information outlined in this affidavit, there is probable cause to believe that items to be seized set forth in Attachment B, which are incorporated by reference in this affidavit, are evidence of the SUBJECT OFFENSES and will be found on the SUBJECT DEVICE. I believe upon the search of the SUBJECT DEVICE that agents/officers will locate evidence including, but not limited to, records from the illegitimate sale of controlled substances, records demonstrating the use of proceeds, contracts, purchasing documents, receipts, travel tickets, loan agreements, title company statements, notes, ledgers, and other assets or financial records related thereto, and other evidence of drug diversion and trafficking, including prescriptions, charts, billing logs, payment records, patient files with fictitious documentation, dispensing logs, invoices, and inventories.

59. The SUBJECT DEVICE is further described in Attachment A, which is incorporated by reference into this affidavit. This section incorporates by reference the above paragraphs.

60. I know from my training and experience that people trafficking in prescription controlled substances, as well as medical professionals in general, commonly use cellular phones and electronic communication to conduct their business, and communicate with their co-conspirators. This is even more true for ROSENFELD as

airline records obtained by DEA reveal he was only in Houston a few days a month, and therefore, had few opportunities to conduct clinic business in person.

61. Pursuant to his status as a DEA registrant, ROSENFELD provided the address of Sunnyside #1 as his practice address in Texas, and included the number associated with the SUBJECT DEVICE as both the number for Sunnyside #1, and his “contact number.” Agents obtained ROSENFELD’s application to become a pain management clinic, dated October 2018, and it listed the number for the SUBJECT DEVICE as his number. Agents obtained information regarding ROSENFELD’s Delta “Sky Miles” account and it lists the number for SUBJECT DEVICE.

62. Since September 2019, when the SUBJECT DEVICE and a copy of its contents were mailed to DEA Houston, the SUBJECT DEVICE has been maintained in an evidence locker at DEA Houston. On October 18, 2019, the SUBJECT DEVICE was removed from temporary storage and added to the inventory in the DEA vault. On December 23, 2019, the SUBJECT DEVICE, logged as non-drug evidence N-85 (referred to on the evidence list as “One iPhone belonging to Dr. ROSENFELD – IMEI:356-172-090-590-826”), was moved from one shelf to another within the evidence vault. There has been no further action since December 23, 2019. There is no reason to believe that the SUBJECT DEVICE has been altered in any way since it was obtained in August 2019.

I. Toll Records

63. Agents obtained toll records for SUBJECT DEVICE, which show dozens of calls to and from Stewart and Taylor during the timeframe of the alleged conspiracy. Specifically, toll records reveal that from on or about January 2, 2019 through on or

about July 12, 2019 there were approximately 307 calls between the SUBJECT DEVICE and Stewart.

II. CI#2 calls with ROSENFELD to SUBJECT DEVICE

64. CI#2 approached Taylor at DEA's direction through a mutual connection and posed as a doctor who wanted to work in a pain clinic. Although most of CI#2's dealings were with Taylor and Stewart, he/she also spoke with ROSENFELD about the position. ROSENFELD showed hesitance to speak in detail about the position because CI#2 did not have an active DEA Registration number and the TMB had posted an agreed order in August 2018 suspending CI#2's medical license (due to CI#2's drug conviction). Despite ROSENFELD, Taylor, and Stewart knowing CI#2 did not have a valid DEA registration number, and that CI#2 had been suspended by TMB from treating chronic-pain patients, they had several discussions with CI#2 about hiring CI#2 at Sunnyside #2, as described in the following paragraphs:

65. On March 22, 2019, CI#2 called ROSENFELD at the number for the SUBJECT DEVICE and said that CI#2 had "good news." CI#2 told ROSENFELD he/she had his/her new DEA number and would it "be okay" if he/she sent ROSENFELD a copy of his DEA number. ROSENFELD said that it was okay, but that his concern was having the TMB order taken off their website. CI#2 assured ROSENFELD that his lawyer was taking care of the issue. CI#2 then attempted to have ROSENFELD give CI#2 more details about how ROSENFELD operated the clinic. ROSENFELD hesitated in talking to CI#2 about the details, and said that he wanted CI#2 to remedy his issue with the TMB first.

66. On April 2, 2019, CI#2 called ROSENFELD at the number for the SUBJECT DEVICE and told ROSENFELD that CI#2 got a letter from his/her attorney showing that his/her

DEA License was not suspended. He/she also said, “I got my letter from TMB that they’re updating the website.” CI#2 added that he/she spoke with Taylor and was “excited to be working with Dr. Kobza.” ROSENFELD told CI#2 to email him the letter from TMB and to make sure TMB’s website was updated and then, “We are good.” CI#2 then again tried to speak with ROSENFELD about the details of how ROSENFELD prescribed at the clinic. CI#2 told ROSENFELD he spoke to Taylor about e-prescribing and asked ROSENFELD to explain how it worked. ROSENFELD told him that after he received confirmation about CI#2’s license, that CI#2 would “sit down with Alantha [Stewart] and she’ll teach you all about that.” This statement corroborates that ROSENFELD relied on Stewart to control his e-prescribing process so that she could e-prescribe controlled substances while ROSENFELD was usually out of the state.

III. Electronic prescribing

67. Additionally, data obtained from ROSENFELD’s electronic prescription provider Surescripts, shows that beginning in or around August 2018, most of ROSENFELD’s prescriptions were electronic prescriptions. I know from my training and experience doctors who e-prescribe, often do so from applications on their cellular phones or from a computer. As described above, Taylor told CI#2 during a conversation recorded by CI#2, that Stewart e-prescribed controlled substance prescriptions from her cellular phone on ROSENFELD’s behalf.

68. On March 22, 2019, CI#2 recorded a meeting with Taylor, Stewart, and Fisher at Sunnyside #1. CI#2 inquired about how Sunnyside prescribed electronically. Taylor responded that the process was easy and that CI#2 would be sent a “hard token” that would be set up on CI#2’s phone, or a key card, to make sure CI#2 is “pushing” the e-

prescriptions through. Stewart also spoke with CI#2 about delegating responsibilities to nurse practitioners. Taylor told CI#2 that CI#2 would hire a nurse and “you make money through her...she can e-scribe for you.” Given that Taylor told CI#2 that they would enable CI#2 to e-prescribe on his phone, and that most of ROSENFELD’s prescriptions were electronically prescribed, it is highly likely that ROSENFELD will have information and applications related to e-prescribing for Sunnyside on SUBJECT DEVICE.

69. Based upon these facts, there is probable cause to believe the SUBJECT DEVICE contains evidence of the crimes discussed above. Accordingly, this affidavit seeks to search the SUBJECT DEVICE.

IV. Probable Cause That Evidence Of Crimes Is On Subject Device Based Upon Training And Experience

70. Based on my training and experience, as outlined above; the facts and circumstances of this investigation; and consultations with experienced narcotics investigators in the DEA and other agencies with extensive knowledge of pharmaceuticals regarding the methods and practices of individuals trafficking in or diverting pharmaceutical controlled substances, I know that persons involved in drug diversion and trafficking, including medical professionals, often maintain and retain on their cellular phones the following:

a. Records⁸ and information relating to bank accounts, certificates of deposit, stocks, mutual funds, and safe deposit boxes that often contain proceeds of illegal activities;

⁸ The term “records,” used throughout this Section, includes all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including computers and any other electrical, electronic, or magnetic form, such as any information on an electronic or magnetic storage device, including CD-ROM’s, optical discs, thumb drives, , smart cards, memory calculators, computer tablets, smart phones, computers, as well as readouts or printouts from any magnetic storage device, any handmade form, any mechanical form, and any photographic form;

b. Proceeds and records of drug sales and transactions; books, account ledgers, records, receipts, notes, journals, ledgers and other documents relating to financial transactions; and records, and information relating to obtaining, transferring, and spending proceeds of drug diversion and trafficking activities;

c. Records that establish control of various premises, including residences and business premises, including utility bills, cancelled checks, envelopes, deeds, leases, titles, and vehicle registrations;

d. Records and correspondence relating to the order of medical equipment and supplies, and business or professional contracts and agreements;

e. Records containing or relating to names, addresses, phone numbers, email addresses, and personal information of coconspirators, associates, subordinates, employees, and others who join, aid, and abet drug diversion and trafficking in address books, electronic organizers, cellular phones and smart phones, diaries, planners, notebooks, and other physical and electronic storage locations;

f. Patient files and records of office visits, progress notes, prescriptions, urine drug testing, referrals and other patient information. I know under Texas law and by regulation, as described further above, physicians are required to keep records of controlled substance prescriptions they write and dispense. In my training and experience, I know that physicians keep these types of patient records on their cellular phones, and in other electronic formats. I also know based on my training and experience that physicians and clinic owners and managers often transport patient records and documents—both in paper and electronic format on laptops and other electronic storage devices—in their vehicles to other locations, including their residences, to review and update these records.

71. I also know through training and experience, that persons involved in drug diversion and trafficking frequently:

a. Use land line telephones and cellular telephones to conduct business. I further know that evidence of these transactions and the identities of coconspirators and others involved in drug diversion and trafficking can be obtained from telephone and cellular telephone bills and statements; as well as from the telephones, cellular telephones, and associated caller identification devices, voicemail, and answering machines. These bills, business notes, letters and correspondence relating to their business statements, as well as the communications devices, are often stored and maintained in residences or on cellular telephones and other areas under the dominion and control of those involved in narcotics trafficking;

b. Attempt to invest their illegal proceeds into legitimate businesses as a means of laundering their drug profits. These organizations often attempt to acquire interest or control of businesses that conduct a large portion of their business in the form of cash and that makes the commingling of drug proceeds with legitimate income an easier task. The

acquisition of these legitimate business interests with drug proceeds often creates documentary evidence in the form of bank records, corporation records, financial statements, loan agreements, partnership agreements, and other evidence that is frequently stored or maintained in areas under the dominion and control of the heads of the criminal organization; and

c. Communicate about their crimes with coconspirators and others using their cellular phones. Persons involved in drug trafficking often keep their cellular phones on their person or in their residence.

V. Computers, Electronic Storage, and Forensic Analysis

72. As described above and in Attachment B this application seeks permission to search for records that might be found on the SUBJECT DEVICE. Thus, the warrant applied for would authorize the review of the previously obtained image of the SUBJECT DEVICE or the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

73. I submit that there is probable cause to believe records will be stored on—and remain on—the SUBJECT DEVICE, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence,

because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

74. Further, the SUBJECT DEVICE is currently in the evidence vault at DEA Houston, located at 1433 West Loop South in Houston, Texas, and has been since September 2019, when it was mailed to DEA Houston from Georgia where the SUBJECT DEVICE was originally seized. I know from training and experience, and from conferring with the evidence vault personnel, that the SUBJECT DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICE first came into the possession of the DEA.

75. As further described in Attachment B, this application seeks permission to locate not only files on SUBJECT DEVICE that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the SUBJECT DEVICE was used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on SUBJECT DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or on a mobile device may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

76. In most cases, a thorough search of a premises for information that might be stored on storage media, such as cellular phones, often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a cellular phone has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers, including cellular phones which are essentially mini-computers, can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

77. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

78. The warrant I am applying for would permit law enforcement to obtain from ROSENFELD the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial

recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of

the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

79. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the government to utilize the image obtained in August 2019 pursuant to the Original Warrant, as there is no reason to believe that image is any different from an image that would be obtained anew. Further, the image obtained pursuant to the Original Warrant in August 2019 went through a filter process to remove potentially privileged information from the prosecution team's possession, and was produced to all defendants in January 2021. In the alternative, the warrant I am applying for would permit the examination of the SUBJECT DEVICE consistent with the warrant anew. This examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

(Continued)

CONCLUSION

80. Based upon the foregoing, probable cause exists to believe that SUBJECT DEVICE contains evidence of the SUBJECT OFFENSES.

Melvinla Morgan

Melvinla Morgan, Diversion Investigator
Drug Enforcement Administration

Subscribed and sworn to via
telephone this 8th day of May, 2023,
and I find probable cause.

Christine A. Bryan

HONORABLE CHRISTINA A. BRYAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is the iPhone associated with phone number 941-456-3635 and IMEI 356172090590826, belonging to Jonathan Rosenfield, M.D. (“ROSENFELD”), currently in the evidence vault, as non-drug exhibit 85, in the custody of the Drug Enforcement Administration (“DEA”) located at 1433 West Loop South, Houston, Texas 77027 (“ROSENFELD DEVICE”). This warrant authorizes the forensic examination of the SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records and information on the SUBJECT DEVICE described in Attachment A that constitute fruits, evidence, and instrumentalities of violations of Title 21 United States Code, Sections 841(a)(1) (unlawful distribution of controlled substances); 846 (conspiracy to unlawfully distribute controlled substances); and 856 (a)(1) (maintaining a drug-involved premises), including but not limited to:

1. Content of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, social media account activity (including browser history, web page logs, and search terms entered by the user), photos, WhatsApp content and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above;
2. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Evidence of the times the devices were used;
4. Passwords, encryption keys, and other access devices that may be necessary to access the devices;
5. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violation described above.

Attachment A to Affidavit in Support of an Application for Search Warrant

Application Checklist

Case Number: _____

☐ Check if emergency

Type of application: (check all that apply)

☐ Standard Form (specify): _____

<input type="checkbox"/> Criminal complaint <input type="checkbox"/> Arrest warrant+ <input checked="" type="checkbox"/> Search/seizure warrant (indicate type of search): <u>phone</u>	<input type="checkbox"/> Administrative inspection warrant <input type="checkbox"/> Forfeiture <input type="checkbox"/> Other (specify): _____
--	--

All fields in warrants must be populated: ie: date; city and state; judge's name and title; date the search warrant expires.

Sworn to

☐ by ☒ in person telephone: use form AO 106A (Application for a Warrant by telephone); and supporting affidavit must indicate that it was sworn to telephonically

Offense specified: (check all that apply)

- | | | | |
|---|---|---|--------------------------------------|
| <input checked="" type="checkbox"/> Drugs | <input type="checkbox"/> Fraud | <input type="checkbox"/> Weapons | <input type="checkbox"/> Immigration |
| <input type="checkbox"/> Sex offenses | <input type="checkbox"/> Theft | <input type="checkbox"/> Kidnapping | <input type="checkbox"/> Tax |
| <input type="checkbox"/> Extortion/Racketeering | <input type="checkbox"/> Fugitive/Escape/Supervised release | <input type="checkbox"/> Computer crime | |
| <input type="checkbox"/> Terrorism | <input type="checkbox"/> Other (specify): _____ | | |

Sealing request: ☒Delayed notice request ☐

Duration: ☐ 30 days ☐ 90 days ☒ 180 days* ☐ Other _____

*Note: no application will be sealed for more than 180 days without a statutory reference or compelling circumstance; proposed order must include the duration. The Court will not sign any proposed orders that do not include the duration.

Grounds: ☐ endangering life or physical safety of individual ☐ flight from prosecution
☒ evidence destruction/tampering ☐ witness intimidation
☐ otherwise seriously jeopardizing investigation or unduly delaying trial
☒ Initial request ☐ Previous extensions (# and date) _____

Has this application been previously submitted for consideration? ☐ Yes ☒ No

Date _____ Action Taken _____ Judge _____

Agent's name: Troy Hunter
DEA TFO

Phone#: 281-932-8145

I certify that the attached has been reviewed for compliance with Rules 3, 4, 4.1, and/or 41 of the Federal Rules of Criminal Procedure and that the standard approved form has not been changed.

AUSA Signature: _____

Phone#: 202-679-1883

Printed Name: Jason Knutson

UNITED STATES DISTRICT COURT

for the
Southern District of Texas

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

ROSENFELD's cell phone with the number
941-456-3635
("SUBJECT DEVICE")

Case No.

H19-1621M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

ROSENFELD's cell phone with the number 941-456-3635, ("SUBJECT DEVICE")

located in the Southern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachments A and B to the Affidavit in Support of Search Warrant.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841	Distribution of Controlled Substances
21 U.S.C. § 846	Conspiracy to Distribute Controlled Substances
21 U.S.C. § 856(a)(2)	Maintaining a Drug-Involved Premises

The application is based on these facts:

See attached Affidavit of Task Force Officer Michael Henson Drug Enforcement Administration

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date:

8/27/19

City and state: Houston, Texas

Troy L. Hunter
 Applicant's signature

Michael Henson Task Force Officer, DEA

Printed name and title

Peter Bray
 Judge's signature

United States Magistrate Judge Peter Bray

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)

ROSENFELD's cell phone with the number
 941-456-3635
 ("SUBJECT DEVICE")

Case No.

H19-1621M

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of Texas
 (identify the person or describe the property to be searched and give its location):

ROSENFELD's cell phone with the number
 941-456-3635
 ("SUBJECT DEVICE")
 See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachments A and B.

YOU ARE COMMANDED to execute this warrant on or before September 4, 2019 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Peter Bray
 (United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued:

8/27/19 8:25pm


 Judge's signature

City and state:

Houston, TexasUnited States Magistrate Judge Peter Bray

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT

I, Troy L. Hunter, being duly sworn, hereby depose and state as follows:

SUMMARY OF THE INVESTIGATION, RELEVANT SUBJECTS, AND PREMISES

1. Elmer Taylor (“TAYLOR”) and his wife Alantha Stewart Taylor (“STEWART”) own or control Sunnyside Medical, PLLC, which does business as Sunnyside Wellness at two locations on Edfield Street (“Sunnyside #1”) and Pinemont Drive (“Sunnyside #2”) in or around Houston, Texas. Jonathan Rosenfield, M.D. (“ROSENFELD”) is the prescribing physician at Sunnyside #1, and the owner on paper, while Paul Kobza, D.O. (“KOBZA”) is the prescribing physician at Sunnyside #2. Ardella FISHER, NP (“FISHER”) is the Nurse Practitioner under ROSENFELD at Sunnyside #1, while Enna AMEDOME, NP (“AMEDOME”) is the Nurse Practitioner under KOBZA at Sunnyside #2. A DEA investigation has revealed that Sunnyside Wellness operates as a pill mill that is participating in the diversion of hydrocodone, oxycodone, and carisoprodol (all controlled substances). The investigation revealed that ROSENFELD used a cell phone with the number 941-456-3635 (“SUBJECT DEVICE”) to communicate with his co-conspirators.

2. On August 21, 2019, grand jury indicted ROSENFELD, STEWART, TAYLOR, FISHER, AMEDOME and others for conspiracy to distribute controlled substances. Agents intend to arrest ROSENFELD, an others, on August 28, 2019 and seek a warrant to search and seize SUBJECT DEVICE during the arrest of ROSENFELD.

IDENTITY AND EXPERIENCE OF AFFIANT

3. I am a Task Force Officer (TFO) assigned to the Drug Enforcement Administration (DEA), Houston Division Office, Tactical Diversion Squad (TDS). The TDS is a multi-agency task force that investigates the illegal trafficking of pharmaceutical controlled substances that is

comprised of agents from the DEA, Internal Revenue Service, Federal Bureau of Investigation, and state and local law enforcement personnel assigned as Task Force Officers (TFOs).

4. I am a licensed Peace Officer in the State of Texas employed by the Texas Department of Public Safety as a Special Agent (SA) in the Criminal Investigations Division who deals with the Texas Penal Code and the Texas Health and Safety Code Laws.

5. I am also a graduate of Texas Southern University, Class of 1989 with a Bachelor of Science in Pharmacy. I not only worked as a licensed pharmacist for nine years, but was a licensed pharmacy technician for six years. I continue to maintain my pharmacy license to practice pharmacy in the State of Texas.

6. I have been assigned to the Texas Department of Public Safety, Methamphetamine Initiative Group (MIG) primarily tasked with the apprehension of individuals involved in the trafficking of methamphetamine throughout the Houston, Texas and surrounding areas. I have also been certified through the DEA with the dismantling and destruction of illegal clandestine laboratories (common known as "meth labs").

7. I have been assigned to the DEA since 2018 and have received specialized training while attending DEA TFO School in Houston, Texas and DEA Tactical Diversion School in Murfreesboro, Tennessee, concerning violations of the Controlled Substances Act within Title 21 of the United States Code.

8. As a SA with the Texas Department of Public Safety and a TFO with the Drug Enforcement Administration I have been a case agent or a participant in numerous narcotics trafficking investigations. I am familiar with smuggling techniques, counter-surveillance techniques and other methods used by narcotics traffickers. I am a graduate of the Texas Department of Public Safety Training Academy in Austin, Texas gaining over twelve hundred

hours of police training. I have received many hours of formal training in the detection and apprehension of persons involved in the trafficking of illegal narcotics. I have received comprehensive, formalized instruction in such matters as narcotics identification, detection, trafficking, and interdiction; money laundering techniques; and asset identification, seizure, and forfeiture, and have received training in the conduct of narcotics enforcement and investigations. I have training and experience in Narcotics Investigations to include surveillance and working with informants and have participated in and has conducted investigations which have resulted in the arrest and conviction of individuals who have smuggled, received, and distributed controlled substances as well as the seizure of illegal drugs and proceeds derived from the sale of those illegal drugs. During my employment with the Texas Department of Public Safety and as a TFO with the DEA, I have participated in numerous narcotics investigations along with other experienced SAs and law enforcement personnel. These investigations have involved: the unlawful importation, manufacture, possession with intent to distribute, and distribution of narcotics (including methamphetamine, cocaine, heroin); the laundering of narcotics proceeds and monetary instruments derived from narcotics activities; and conspiracies associated with narcotics offenses. These investigations have also involved debriefing defendants, witnesses, and informants; recruiting and directing informants; conducting surveillance and telephone toll analysis; conducting wire intercept investigations, and applying for and executing state and federal search warrants. Many of these investigations have resulted in the seizure of narcotics and narcotics-related assets, and arrests for narcotics-related offenses.

9. Since November 2018, I have been assigned to the Houston Division Office Tactical Diversion Squad (TDS), which is tasked solely with the investigation of the illegal trafficking of pharmaceutical controlled substances, often referred to as "diversion." Through my

position, I have spoken with pharmacists, physicians, diversion investigators, state medical board investigators, pharmacy board investigators, patients and other witnesses with extensive knowledge of pharmaceuticals, regarding the methods and practices of individuals trafficking in or diverting pharmaceutical controlled substances.

10. During my time at TDS and Texas Department of Public Safety, I have become familiar with pain management clinics that prescribe large quantities of controlled substances to people known to be diverting the controlled substances for illegitimate gain. These clinics are often referred to as “pill mills.” I know from prior investigations that the pain management clinics often prescribe large quantities of oxycodone, hydrocodone, and carisoprodol without a legitimate medical purpose and outside the course of professional practice.

PURPOSE OF THE AFFIDAVIT

11. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search SUBJECT DEVICES more particularly described in ATTACHEMENT A.

12. Based on my training, experience, and the facts set forth in this Affidavit, I have probable cause to believe that Elmer TAYLOR, Alantha STEWART, Dr. Jonathan ROSENFELD, Ardella FISHER, Paul KOBZA, Enna AMEDOME,, and others known and unknown to the investigation have committed violations of the Controlled Substances Act, including: 21 U.S.C. § 841 (Distribution of Controlled Substances); 21 U.S.C. § 846 (Conspiracy to Distribute Controlled Substances), 21 U.S.C. § 856(a)(2) (Maintaining a Drug-Involved Premises). I also have probable cause to believe that SUBJECT DEVICE, more particularly described below and as set forth in ATTACHMENT A, contains evidence, instrumentalities, and fruits of these crimes, more particularly described in ATTACHMENTS B.

13. The information in this affidavit is derived from my participation in this investigation and information obtained from several sources, including: Oral and written reports about this and other investigations, which I received from various federal and local law enforcement agencies; physical surveillance and undercover operations conducted by investigators in which I participated directly or that were directly or indirectly reported to me; telephone toll records, public sources, and business records; information from a medical doctor who is an expert in the field of pain management; and information from Confidential Informants (CI#1, CI#2, CI#3, CI#4¹), which was only relied upon once it had been deemed reliable through independent corroboration of information provided,² and undercover DEA Agents.

14. Because this affidavit is submitted for the limited purpose of securing authorization for a search and seizure warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are essential to establish the necessary foundation for the requested search warrant.

BACKGROUND

I. Relevant Statutes and Regulations

15. 21 U.S.C. § 841(a)(1) makes it unlawful for any person to knowingly and intentionally distribute or dispense a controlled substance except as authorized by law. A medical professional violates this statute by knowingly and intentionally distributing or dispensing a

¹ CI#1, CI#3, CI#4 are confidential informants paid by the DEA. CI#2 is a cooperating defendant that is seeking credit for his/her cooperation.

²While not all information provided by CIs could be independently corroborated, sufficient information from the CIs was corroborated and could be relied upon. Based on my training, experience, and knowledge of the facts of the investigation, I believe that the CIs used in this case are reliable. The CIs used in this case provided information to law enforcement for various reasons including monetary compensation.

controlled substance for no legitimate medical purpose and not in the usual course of professional medical practice. *United States v. Rosen*, 582 F.2d 1032, 1034 (5th Cir. 1978).

16. 21 U.S.C. § 846 prohibits an agreement between two or more persons to unlawfully distribute or dispense controlled substances.

17. 21 U.S.C. § 856(a)(1) makes it unlawful to “knowingly open, lease, rent, use, or maintain any place, whether permanently or temporarily, for the purpose of manufacturing, distributing, or using any controlled substance.”

18. According to 21 C.F.R. § 1306.14, every person who dispenses a controlled substance must be registered to do so with the DEA. 21 C.F.R. § 1306.04(a) further provides:

A prescription for a controlled substance to be effective must be issued for a legitimate medical purpose by an individual practitioner acting in the usual course of his professional practice. The responsibility for the proper prescribing and dispensing of controlled substances is upon the prescribing practitioner

19. Both federal and state law provide for the maintenance of medical records and inventory. 21 C.F.R. § 1304.04 requires registrants to keep, and to make available to the DEA for inspection and copying, medical records and inventory for at least two years from the inventory or record date. In addition, 22 Texas Administrative Code § 165.1 requires physicians licensed by the Texas Medical Board (“TMB”) to maintain complete, contemporaneous, and legible patient records that document each patient encounter with respect to (1) the “reason for the encounter and relevant history, physical examination findings, and prior diagnostic test results;” (2) an “assessment, clinical impression, or diagnosis;” (3) a “plan of care,” including, if appropriate, a plan for discharge; and (4) the “date and legible identity of the observer.”

20. 21 U.S.C. § 822 states that, aside from some exceptions not relevant here, controlled substances may only be prescribed, dispensed, or distributed by persons registered with the DEA. *See also* 21 C.F.R. § 1306.04.

21. The Prescription Monitoring Program (“PMP”) is a database of all reported prescriptions for controlled substances that are issued and dispensed in Texas.

22. Both federal and state law provide for the maintenance of pharmacy records and inventory. *See, e.g.*, 21 C.F.R. § 1304.04 (records must be maintained at least two years from the inventory or record date); 22 Texas Admin. Code § 291.34(a)(1)(A) (establishing same requirement of Texas pharmacies).

II. Relevant Controlled Substances

23. 21 U.S.C. § 812 establishes five schedules of controlled substances—Schedules I, II, III, IV, and V—based on the drug’s potential for abuse, its currently accepted medical use, and the severity of physical or psychological dependence that could result from its abuse. Pharmaceutical controlled substances are listed in Schedules II through V because they are considered drugs for which there is an accepted medical use, but which pose a substantial potential for abuse and addiction. Relevant here,

a. **Oxycodone** is the generic name for a Schedule II analgesic drug that is typically prescribed for moderate-to-severe pain relief. Due to its potential for addiction, oxycodone prescriptions are generally issued for a modest number of pills to be taken over a short period of time. Oxycodone is a commonly abused and diverted controlled substance.

b. **Hydrocodone** is the generic name for a narcotic analgesic that was reclassified from a Schedule III to a Schedule II controlled substance as of October 6, 2014. Hydrocodone is sold under several brand names, including Norco. Hydrocodone is a commonly abused and diverted controlled substance.

c. **Carisoprodol** is a Schedule IV controlled substance. It is classified as a muscle relaxant. According to the Food and Drug Administration (“FDA”), carisoprodol should only be used for acute treatment periods of up to two to three weeks. According to recent expert testimony in a similar case, I know that carisoprodol is “a drug of abuse without any proof of efficacy.” Additionally, when taken with oxycodone or hydrocodone,

carisoprodol can cause an increased sensation of euphoria, which increases its potential for abuse and risk of death.

III. The illegal process of diverting prescription drugs

24. Based upon my training and experience, illegal pain management clinics and pharmacies that operate as “pill mills” are generally comprised of owners and operators; physicians, pharmacists, and other medical providers; and office staff.

25. A “crew leader” is usually someone who finds and pays individuals, some of whom are homeless or impoverished, to pose as chronic pain patients; transports them (often in groups) to the clinic; coach the patients to fill out patient intake documentation to support a prescription for pain medication and pays for the “visit with the doctor” (i.e., the illegitimate prescription); takes the patient (or just the illegitimate prescription) to the pharmacy; and pays for and takes control of the prescription drugs, often to divert and sell them on the street for profit.

26. Often, the clinic and pharmacy owners/operators coordinate with the crew leaders to set aside appointments for individuals the crew leaders bring to the clinic. The clinic often charges a flat fee, paid up front—before the patient sees the physician—usually in cash, based on the controlled substance the physician will later prescribe. For example, a patient might pay \$300 at the beginning of a visit knowing the resulting prescription will be for hydrocodone, or \$500 at the beginning of a visit, knowing the resulting prescription will be for oxycodone.

27. The actual doctor visit—if any—usually includes only a perfunctory consultation. At the conclusion of the visit, the physician almost always orders a Schedule II opioid, such as hydrocodone or oxycodone, and routinely a second for a Schedule IV drug such as alprazolam (a drug used to treat anxiety) or carisoprodol. These prescriptions are issued without a legitimate medical purpose and outside the scope of professional practice.

28. Some pharmacies require each “patient” to present his/her own prescription; others allow crew leaders to present the patients’ IDs for copying. The crew leaders (whether directly or through their “patients”) usually pay in cash, even if they have insurance, which allows the pharmacy to charge above-market rates without leaving a paper trail for insurance providers, including private insurance, Medicare, and Medicaid; and by DEA and other law enforcement. For example, according to pharmacists with knowledge of market rates, legitimate pharmacies may charge \$42.00 for 120 dosage units of oxycodone 30mg and \$6.00 for 90 dosage units of carisoprodol 350mg, while pill-mill pharmacies will charge as much as \$1,340 for that combination. These prices reflect the high market value of the drugs on the illegal drug market.

29. Based on my training and experience, I know that “pill mill” clinics and pharmacies often attempt to avoid detection by law enforcement by: falsifying patient records and prescriptions, accepting a combination of pain management and family medicine patients, requiring appointments, requiring patients to have prior prescriptions for controlled substances on the PMP, papering patient files with x-ray or MRI results that are rarely reviewed or verified, maintaining irregular business hours, depositing only a portion of the cash proceeds in the bank.

PROBABLE CAUSE OF VIOLATIONS OF LAW

30. A grand jury sitting in the Southern District of Texas found probable cause that the Defendants and others are involved in prescribing controlled substances without a legitimate medical purpose and outside the usual course of professional practice. Additionally, probable cause exists to believe that the SUBJECT DEVICE, contains evidence of ROSENFIELD’s illegitimate prescribing practices, and evidence that the TARGETS violated various federal drug trafficking laws, including 21 U.S.C. § 841(a)(1) (Distribution of Controlled Substances); 21 U.S.C. § 846 (Conspiracy to Distribute Controlled Substances); and 21 U.S.C. § 856(a)(2)

(Maintaining drug-involved premises), Also, probable cause exists to believe that evidence, fruits, and instrumentalities of the above-described violations will be found during the search of SUBJECT DEVICES.

31. DEA began investigating TAYLOR and STEWART in or around January 2018 as part of its focus on targeting illegal pain management clinics, pharmacies, and physicians in the Houston area.

32. During the course of the investigation, CIs and undercover agents visited SUNNYSIDE #1 and #2. Through their in-person visits, footage obtained through video surveillance directed at both SUNNYSIDE #1 and #2, surveillance, photos, PMP data, and other investigative tools, agents have learned that SUNNYSIDE operates as a pill mill. The following “red flags” have been observed at SUNNYSIDE #1 and #2:

a. Individuals—posing as patients—are often brought to SUNNYSIDE in groups by “crew leaders.” These crew leaders often sit in their cars in the parking lot until their patients are ready to be brought into the clinic. Surveillance showed many of the same vehicles parked in SUNNYSIDE parking lots on several occasions. Several CIs familiar with pill mills visited SUNNYSIDE and observed known crew leaders bring individuals posing as patients to SUNNYSIDE.

b. SUNNYSIDE #1 and #2 do not accept insurance; it is an all-cash business. SUNNYSIDE, charges \$200 to \$300 for hydrocodone and carisoprodol and between \$400 and \$500 for oxycodone and carisoprodol. Individuals seeking prescriptions pay cash *before* seeing the physician based on the prescription they will later receive from ROSENFELD or KOBZA.

c. SUNNYSIDE #1 and #2 employ several armed security guards in the parking lot and inside the clinic. These guards control patient flow and help enforce SUNNYSIDES’ rules.

d. The majority of individuals who visit SUNNYSIDE posing as patients are prescribed the same or similar combinations of controlled substances with the same or similar dosage units, notwithstanding the patients varied characteristics (age, weight, sex, medical history, diagnosis, etc.). Most often, the patients are prescribed the highest strength pills of short-acting oxycodone, hydrocodone, and carisoprodol available on the market.

I. Relevant Individuals

33. Elmer TAYLOR owns and operates Sunnyside Wellness, located at the SUNNYSIDE #1 and #2. TAYLOR also recruits patient-runners and purported patients to buy controlled substances not for a legitimate medical purpose and outside the course of professional conduct.

34. Alantha STEWART is married to TAYLOR and also owns and operates Sunnyside Wellness. According to Texas Secretary of State Records, STEWART formed SUNNYSIDE WELLNESS CENTER, LLC on May 17, 2018. Those records list STEWART as the Manager.

35. Jonathan ROSENFELD, a resident of Atlanta, Georgia, is a Medical Doctor, and has been licensed to practice medicine in the State of Texas since in or around December 2017. ROSENFELD maintains a DEA Registration Number, which allows him to prescribe Schedule II through V controlled substances. ROSENFELD is the purported owner of SUNNYSIDE #1 and the Medical Director at SUNNYSIDE #2. According to PMP records and the investigation, ROSENFELD prescribes large volumes of controlled substances—primarily oxycodone 30mg, hydrocodone 10/325mg, and carisoprodol 350mg—out of SUNNYSIDE without a legitimate medical purpose and outside the usual course of professional conduct.

36. Ardella FISHER has been a Family Nurse Practitioner licensed to practice in the State of Texas since in or around November 2017. As a Nurse Practitioner, FISHER is able to prescribe Schedule III through V controlled substances, and maintains a DEA Registration Number. According to TMB, ROSENFELD is FISHER's supervising physician. FISHER purports to treat patients for pain at SUNNYSIDE #1.

37. Paul KOBZA is a Doctor Osteopathic Medicine, and has been licensed to practice in the State of Texas since in or around August 2002. KOBZA maintains a DEA Registration

Number, which allows him to prescribe Schedule II through V controlled substances. KOBZA is purportedly the physician at SUNNYSIDE #2 and, according to PMP and the investigation, prescribes large volumes of controlled substances—primarily oxycodone 30mg, and hydrocodone 10/325mg, out of SUNNYSIDE #2 without a legitimate medical purpose and outside the usual course of professional conduct.

38. Enna AMEDOME is a Family Nurse Practitioner licensed to practice in the State of Texas since in or around November 2017. As a Nurse Practitioner, AMEDOME is able to prescribe Schedule III through V controlled substances, and maintains a DEA Registration Number. According to TMB, KOBZA is AMEDOME's supervising physician. AMEDOME purports to treat patients for pain at SUNNYSIDE #2.

II. Specific Instances of Illegal Conduct at SUNNYSIDE #1

A. CI#1

39. In mid-July 2018, CI#1 visited SUNNYSIDE #1 and obtained TAYLOR's phone number (832-452-1996) from a worker at Sunnyside #1. On or about July 20, 2018, CI #1 met with TAYLOR at SUNNYSIDE #1, and made a consensual recording. During the meeting, CI#1 asked TAYLOR if CI#1 could purchase oxycodone prescriptions. TAYLOR told CI #1 that "my doctor" was in Canada and that CI#1 might not be able to obtain the prescriptions until Monday. CI#1 asked TAYLOR what TAYLOR charged, and TAYLOR told CI#1 it was "three" for "Norco" and "five" for "Oxy." TAYLOR also told CI#1 the amounts would be "120 and 90." TAYLOR showed CI#1 a prescription and said it would be "112 [pills]" or something close to that number. CI#1 agreed with TAYLOR to buy the pills "on Monday." CI#1 asked if he/she could just bring IDs. TAYLOR responded for CI#1 to bring IDs and that "we ah ... write it out."

40. Based on my training and experience, and my involvement in the investigation, I know that TAYLOR's doctor—which he referred to as "my doctor"—is ROSENFELD. I also

know that pill mills commonly charge \$300 for hydrocodone and \$500 for oxycodone, and that “120 and 90” refers to the dosage units (number of pills) prescribed on one prescription—120 hydrocodone or oxycodone, and 90 carisoprodol, which are common amounts often prescribed by pill mills. I know that when CI#1 asked if he/she could bring IDs, he/she was asking to bring identification cards only—not the actual “patients” themselves. I know that when TAYLOR told CI#1 that “we ah...write it out” that TAYLOR meant he and others would fill in the name of the person, as well as, the drug and quantity on each prescription.

41. The next Monday, July 23, 2018, CI #1 made a consensually recorded call to TAYLOR. During the call, CI#1 asked TAYLOR, “you got my shit huh?” and told TAYLOR to “give [him/her] three oxys and one Norc.” When CI#1 asked about the price, TAYLOR responded, “my oxys and Soma are \$500, and my Norcos and Somas are \$300.” CI#1 and TAYLOR agreed to meet the next day.

42. As agreed, on Tuesday, July 24, 2018, CI#1 made a consensually recorded visit to meet with TAYLOR at SUNNYSIDE #1. During the meeting, TAYLOR called “Alantha” on the phone—believed to be Alantha STEWART—and told her to bring six “oxys” to the clinic. TAYLOR made another call and directed the listener to “bring the prescription pad.” Soon, STEWART walked into the office at SUNNYSIDE #1 with another lady wearing scrubs, later identified as Shawneece Deyampert.³ CI#1 handed STEWART several ID’s.⁴ STEWART acknowledged, “all this.” The video does not show exactly what they are writing, but from the context of the video, it appears that STEWART and Deyampert are writing on prescriptions and other paperwork, believed to be false patient files. CI#1 then counted out \$3,000 on STEWART’s

³ According to the investigation, Deyampert is an office employee at Sunnyside #1. Deyampert does not have a DEA registration authorizing her to prescribe controlled substances.

⁴ The IDs were provided by law enforcement.

desk while Deyampert and STEWART watch. After the cash is counted, STEWART hands the prescriptions to CI#1 in exchange for the cash.

43. Agents later obtained these prescriptions from CI#1, and confirmed that STEWART gave CI#1 six prescriptions for oxycodone 30mg and 6 prescriptions for carisoprodol 350mg—each purportedly issued by ROSENFELD. Each “patient”—an individual listed on an ID—was issued a nearly identical prescription for between 110 and 114 dosage units (pills) of oxycodone 30mg and 90 dosage units of carisoprodol 350mg. I know, based on my training and experience, and my participation in this investigation, that neither TAYLOR, STEWART, nor Deyampert is a medical professional licensed to practice medicine in the State of Texas.

44. On or about September 17, 2018, CI#1 made a consensually recorded call to TAYLOR and told him she needed to buy some prescriptions. TAYLOR told CI#1 that “I thought you needed like 20 or something...we only doing big shit right now.” CI#1 responded that he/she needed “oxy” and asked TAYLOR if he would give CI#1 a price cut if he/she did “20.” TAYLOR agreed and says that he would take “65.”

45. Based on my training and experience, and my participation in this investigation, I know that “20” means twenty patients (or prescriptions for that many IDs). I also know that “65” likely refers to \$6,500, which represents a discounted rate for 20 prescriptions for oxycodone.

B. CI#3

46. CI#3 told agents that on May 16, 2019, before CI#3 became a confidential source, he/she was paid \$70 by a runner to go to SUNNYSIDE #1 to obtain a prescription for hydrocodone. CI#3 said that he/she was seen by FISHER. CI#3 told agents that he/she told the nurse that he/she had lower back pain. CI#3 described to agents that during the patient visit, FISHER only asked for him/her to breathe in and out and did not perform a physical examination. CI#3 told agents

that CI#3 gave a copy of his/her ID to a runner to fill the prescriptions, and that CI#3 did not fill or receive the prescriptions himself/herself. PMP data corroborates that on May 16, 2019, a pharmacy filled 110 dosage units of hydrocodone 10/325mg purportedly issued to CI#3 by ROSENFELD. Based upon my training and experience I know that FISHER's purported "treatment" of CI#3 was outside the course of professional practice. Additionally, as a Nurse Practitioner FISHER cannot prescribe Schedule II controlled substances.

C. UC#1

47. On or about May 30, 2019, UC#1 made a consensually recorded visit to SUNNYSIDE #1 to obtain prescriptions for controlled substances. UC#1 told agents that there were about six to eight other people waiting. UC#1 presented to the front desk a fake ID that bore a photograph of another person. At some point UC#1 was called to the back where he/she entered an exam room and had an encounter with an unidentified female ("UF") who sat at a computer. The UF asked UC#1 was it his/her first "time here" and UC#1 responded "yes." The UF then asked "do you have the payment on you...?" UC#1 stated, "I do how much is it?" The UF stated, "400 you want oxy's?" UC#1 stated, "Yes" and then UF stated, "400." UC#1 asked the UF, "Do I get soma too or just oxy?" The UF stated, "Just oxy." The UF asked UC#1 several questions regarding her/his health. UC#1 responded that he/she had high blood pressure, shortness of breath, family history of heart problems, and that he/she drinks and smokes.

48. The UF asked UC#1 if he/she wanted "oxycodone" and to which pharmacy UC#1 wanted it sent. UC#1 replied that he/she did want oxycodone and that he/she wanted it sent to a specific Houston-area Pharmacy. The UF told UC#1 the price would be \$400. UC#1 paid \$400 cash and the UF placed the cash in her pocket.

49. UC#1 asked the UF if her boss was a man or a woman and the UF stated, “a woman.” UC#1 asked whether she “is it the doctor,” and the UF replied, “No.” UC#1 later observed Shawneece Deyampert, another armed security guard, and surveillance cameras while seated in the back waiting room.

50. UC#1 was seen by someone who identified herself as “Betty.” UC#1 asked Betty if she was the doctor and she stated, “No, I’m the next best thing.” UC#1 told Betty that he/she had shoulder and neck pain. Betty checked UC#1’s breathing and had UC#1 pull his/her leg out and push it against Betty’s hand. UC#1 asked Betty, whether, when he/she visited the clinic, “I don’t need to see the doctor[?]” Betty said, “No you will see me or somebody like me...it’s rare...[the remainder of the sentence is unintelligible].”

51. UC#1 told agents that he/she did not see ROSENFELD at the clinic, but heard his name mentioned. UC#1 did not have any real injuries. UC#1 did not act as though he/she was in pain. A review of the video shows that the physical exam lasted approximately 1 minute and 4 seconds, and the full visit with Betty lasted approximately 7 minutes and 20 seconds. I know from my training and experience, a \$400 fee for a seven-minute visit of low complexity, is far above market value and inconsistent with the price of a typical physician office visit at a legitimate clinic. The \$400 cash price, however, is consistent with the price pill mills charge for a controlled substance prescription for oxycodone. I know from my training and experience that “Betty’s” purported “treatment” of UC#1 fell outside the usual course of professional practice.

52. On or around June 10, 2019, UC#2 filled the prescription for UC#1, using the same fake ID⁵ that UC#1 used. UC#2 obtained 110 dosage units of oxycodone 30mg. The pill bottle listed ROSENFELD, practicing at SUNNYSIDE #1, as the prescriber. The PMP corroborates that

⁵ The ID used by both UC#2 and UC#1 was an ID issued by DPS that bore the photograph of UC#2.

ROSENFELD purportedly issued an electronic prescription for 110 dosage units of oxycodone 30mg to UC#1. Additionally, a review of records from the TMB, shows that “Betty” is not listed as a Nurse Practitioner under the supervision of ROSENFELD.

III. Meetings with CI#2 at SUNNYSIDE #1 about working at SUNNYSIDE #2

53. On or about February 2, 2019, CI#2 met with TAYLOR, STEWART, and FISHER at a restaurant in Houston to discuss CI#2 working at SUNNYSIDE #2 as a medical professional. At the meeting TAYLOR told CI#2 that the clinic had made “a million dollars” in the past nine months at the clinic. TAYLOR also told CI#2 that FISHER wrote prescriptions for Soma (carisoprodol) and that ROSENFELD gave STEWART the access code to ROSENFELD’s electronic prescribing so that STEWART could prescribe under ROSENFELD’s name from her cell phone. TAYLOR told CI#2 that they sometimes they use Pharmacy A to fill some of their prescriptions, and that Pharmacy A does not report everything to the pharmacy board.

54. On March 22, 2019, CI#2 recorded another meeting with TAYLOR, STEWART and FISHER at SUNNYSIDE #1 to discuss CI#2 working at SUNNYSIDE #2. During the meeting, TAYLOR told CI#2 that, “We 100% certified with the state...so your license will be protected.” TAYLOR told CI#2 that Sunnyside Wellness was “franchised” and that 5400 Pinemont (SUNNYSIDE #2) would also be called SUNNYSIDE WELLNESS, and would be ready to go soon. CI#2 also inquired about prescribing electronically (“e-prescribe”). TAYLOR responded that the process was easy and that CI#2 would be sent a “hard token” that would be set up on CI#2’s phone, or a key card, to make sure CI#2 is “pushing” the e-prescriptions through. STEWART also spoke with CI#2 about delegating responsibilities to nurse practitioners. TAYLOR told CI#2 that CI#2 would hire a nurse and “you make money through her...she can e-scribe for you.”

55. Based on my training and experience, and my participation in this investigation, I know that when TAYLOR referenced that SUNNYSIDE #2 was “certified with the state,” he was referring to its status as a registered pain clinic, which is required if a clinic prescribes more than 50% pain medication. But simply registering as a pain clinic does not allow physicians or clinics license to prescribe outside the scope of professional practice or without a legitimate medical purpose. According to the Texas Medical Board, a pain management certification is location specific and is not transferable to other locations. Based on this information, SUBEJCT PREMISES #1 is a registered certified pain management clinic since February 2019 and SUNNYSIDE #2 is not a registered certified pain management clinic. I also know that in the State of Texas, nurse practitioners are not allowed to e-scribe Schedule II drugs for a physician, nor is a nurse practitioner allowed to prescribe Schedule II drugs for a physician even after an in-person patient visit.

IV. Specific Instances of Illegal Conduct at SUNNYSIDE #2

D. CI#3

56. On or about June 26, 2019, CI#3 made a consensually recorded visit to SUNNYSIDE #2 to obtain prescriptions for controlled substances. CI#3 stated when he/she entered the clinic there were not a lot of people in the front waiting area. CI#3 stated he/she talked with an unidentified black male (“UBM”) that who was sitting in the front waiting area and told CI#3 that earlier in the day there were a lot of people. CI#3 stated the (“UBM”) told him/her that he goes to the doctor for someone and that he is paid \$100.

57. CI#3 stated, while inside the clinic, another unidentified black male introduced himself as Nayda and told CI#3 that he is a recruiter and that he pays \$100 for people to go to the doctor.

58. CI#3 stated when he/she was called to the back that he/she had to give a urine sample and later he/she gave the urinalysis sample, to black female office employee by the name of Ruth LNU. CI#3 stated Ruth did not take his/her blood pressure and that he/she paid \$460 cash for the visit to Ruth. CI#3 stated Ruth told him/her that \$60 was for physical therapy.

59. CI#3 said that he/she was later seen by AMEDOME. CI#3 stated he/she told the clinic he/she had lower back pain. CI#3 described to agents that AMEDOME only asked for him/her to breathe in and out and did not perform a physical examination.

60. CI#3 stated he/she observed two armed security guards at the clinic and one of them was a big black male. CI#3 stated in the back waiting area, he/she observed security cameras on the inside/outside of the clinic almost set up like “the one on Cullen” which is the location of SUNNYSIDE #1.

61. CS#3 stated after his/her visit with AMEDOME he/she was told that he/she had to do physical therapy. CI#3 stated while he/she was waiting for physical therapy that he/she observed another unidentified black male, walk up and tell about 4-5 people or more that were waiting on physical therapy, “come on we don’t need it.” CI#3 stated the people got up and left with the unidentified black male. CI#3 stated shortly thereafter he/she got up and departed as well.

62. A review of the audio of CI#3’s visit shows that the physical exam lasted approximately 21 seconds, and the full visit with AMEDOME lasted approximately 2 minutes. I know from my training and experience, a \$400 fee for a 2-minute visit of low complexity, is far above market value and inconsistent with the price of a typical physician office visit at a legitimate clinic. The \$400 cash price, however, is consistent with the price pill mills charge for a controlled substance prescription for or oxycodone. Based upon my training and experience, I know that AMEDOME’s purported “treatment” of CI#3 fell outside the usual course of professional practice.

63. On or about July 5, 2019, agents had CI#3 fill the prescription issued by KOBZA to CI#3 for 115 pills of oxycodone 30mg at a local pharmacy for \$1,000.

E. CI#4

64. On or about June 26, 2019, CI#4 made a consensually recorded visit to SUNNYSIDE #2 to obtain prescriptions for controlled substances. CI#4 stated when/she entered the clinic he/she sat in the front waiting area. CI#4 stated when he/she was called to the back that he/she went into an exam room where two black females entered the room. CI#4 later identified one of the black females, as Deija Wright⁶. CI#4 stated his/her blood pressure and weight was taken. CI#4 stated he/she was asked some medical history questions.

65. CI#4 stated he/she was asked “What is your pain level 1 through 10?” CI#4 stated “twelve” jokingly. CI#4 was told “A ten, that’s pretty much want to say a 10.” CI#4 was then asked “Who you here with are you here with someone today?” CI#4 stated, “No, I’m here by myself.” CI#4 was asked, “You here by yourself really or did someone bring you here?” CI#4 stated, “By myself.” Deija Wright stated, “You have to pay me for your visit today?” CI#4 stated, “Yes,” Deija Wright asked, “What you gettin?” CI#4 stated, “Norco and Soma.” Deija Wright stated “Norcos is \$300.” CI#4 later paid Deija Wright \$300. I know from my training and experience that it is outside of the usual course of professional practice for a clinic to ask a patient “what you getting” before they are examined by a doctor—especially when considering they are prescribing highly addictive controlled substances.

66. After CI#4 paid the money, he/she sat in the back waiting area where he/she could see the security camera screens on a big television. CI#4 also observed a black male armed security guard.

⁶ Deija WRIGHT is an employee at Sunnyside Wellness #2

67. CI#4 stated later, Deija Wright approached him/her with a computer asking for his/her signature. CI#4 stated, “No” jokingly. Deija Wright stated “it’s just consent stating that you cannot sell or trade any medication that you are prescribed.” CI#4 asked “Why?” Deija Wright stated “Cause you can’t.”

68. CI#4 said later he/she was seen by a black female. CI#4 later identified the black female as Nurse Practitioner AMEDOME. CI#4 stated he/she told the clinic he/she had lower back pain. CI#4 described to agents that AMEDOME only asked for him/her to breathe in and out, squeeze her finger which lasted approximately 35 seconds. AMEDOME did not perform a physical examination. The entire encounter with AMEDOME lasted approximately 2 minutes and 10 seconds. As CI#4 exited he/she observed about 10-12 people sitting in the front waiting area.

69. A review of the video shows that the physical exam lasted approximately 32 seconds, and the full visit with AMEDOME lasted approximately 2 minutes and 15 seconds. I know from my training and experience, a \$300 fee for a two-minute visit of low complexity, is far above market value and inconsistent with the price of a typical physician office visit at a legitimate clinic. The \$300 cash price, however, is consistent with the price pill mills charge for a controlled substance prescription for hydrocodone. Based upon my training and experience, I know that AMEDOME’s purported “treatment” of CI#4 fell outside the usual course of professional practice.

70. SUNNYSIDE #2 sent CI#4’s prescription to CORNERSTONE RX PHARMACY to fill the prescription, and CI#4 received 114 pills of oxycodone 30mg issued by KOBZA. (The prescription bottled indicated CI#4 received 115 oxycodone 30mg pills.) CI#4 also received two prescriptions issued by AMEDOME for non-controlled substances.

V. PMP Data

71. ROSENFELD’s and KOBZA’s prescription patterns support that Sunnyside Wellness located at the SUNNYSIDE #1 and #2 are operating outside the usual course of

professional practice, as their prescribing habits are more consistent with running a “pill mill” than a legitimate medical practice. Moreover, most of the prescriptions issued by ROSENFELD and KOBZA were issued electronically.

72. According to the PMP, from approximately, from in or around May 2018 to August 12, 2019, ROSENFELD issued prescriptions for almost 1.8 million controlled substance pills—approximately 739,000 of those pills were oxycodone. Almost all of these were for 30 milligram pills of oxycodone—the most potent short-acting oxycodone pill available on the market. 91% of all of the pills prescribed by ROSENFELD were for either oxycodone, hydrocodone, or carisoprodol, and many of the prescriptions were dangerously combined with each other. Almost all of the prescriptions for these three drugs were for the highest strengths available on the market.

DRUG NAME	PILLS	% OF TOTAL
Oxycodone 30mg	739,377	41%
Carisoprodol 350mg	495,786	28%
Hydrocodone 10/325mg	398,592	22%
TOTAL	1,896,266	91%

73. From April 8, 2019 to August 12, 2019, while KOBZA was the supervising physician of SUNNYSIDE #2, KOBZA issued prescriptions for a total of 352,193 pills of oxycodone 30mg. The data shows that 82% of KOBZA’S controlled substance prescriptions were for the oxycodone 30mg. Similar to ROSENFELD, KOBZA almost always prescribed the highest available dosages of oxycodone (30mg) and hydrocodone (10/325mg).

DRUG NAME	PILLS	% OF TOTAL
Oxycodone 30mg	352,193	82%
Hydrocodone 10/325mg	51,822	12%
TOTAL	404,015	94%

**PROBABLE CAUSE TO BELIEVE THAT EVIDENCE OF CRIMES IS LOCATED AT
THE SUBJECT DEVICE**

74. Based on evidence derived from the investigation and information outlined in this affidavit, there is probable cause to believe that items to be seized set forth in Attachment B which are incorporated by reference in this affidavit, are evidence of these crimes and will be found on SUBJECT DEVICES. I believe upon the search of the SUBJECT DEVICE that agents/officers will locate evidence including, but not limited to, records from the illegitimate sale of controlled substances, records demonstrating the use of proceeds, contracts, purchasing documents, receipts, travel tickets, loan agreements, title company statements, notes, ledgers, and other assets or financial records related thereto, and other evidence of drug diversion and trafficking, including prescriptions, charts, billing logs, payment records, patient files with fictitious documentation, dispensing logs, invoices, and inventories.

VI. Probable Cause to Believe That Evidence of Crimes Is Located On SUBJECT DEVICE

75. SUBJECT DEVICE is further described and depicted in Attachment A, which is incorporated by reference into this affidavit. This section incorporates by reference the above paragraphs.

76. I know from my training and experience that persons trafficking in prescription controlled substances, as well as medical professionals in general, commonly use cellular phones and electronic communication to conduct their business, and communicate with their co-conspirators. This is even more true for ROSENFELD as airline records obtained by DEA reveal he was only in Houston for a few days a month, and therefore, had few opportunities to conduct clinic business in person.

77. Pursuant to his status as a registrant with the DEA, ROSENFELD provide the address of SUNNYSIDE #1 as his practice address in Texas, and included the number for SUBJECT DEVICE as both the number for SUNNYSIDE #1, and his "contact number." Agents

obtained ROSENFELD's application to become a pain management clinic, dated October 2018, and it listed the number for SUBJECT DEVICE as his number. Agents obtained information regarding ROSENFELD's Delta "Sky Miles" account and it lists the number for SUBJECT DEVICE.

A. Toll Records

Additionally, agents obtained toll records for SUBJECT DEVICE which shows calls to and from SUBJECT DEVICE, and it revealed from in or around January 2, 2019 to July 12, 2019 there were 307 calls between SUBJECT DEVICE and STEWART.

A. CI#2 calls with ROSENFELD to SUBJECT DEVICE

78. CI#2 approached TAYLOR at DEA's direction through a mutual connection and posed as a doctor who wanted to work in a pain clinic. Although most of CI#2's dealings were with TAYLOR and STEWART, he/she also spoke with ROSENFELD about the position. ROSENFELD showed hesitance to speak in detail about the position because CI#2 did not have an active DEA Registration number and the TMB had posted an agreed order in August 2018 suspending CI#2's medical license (due to CI#2's drug conviction). Despite ROSENFELD, TAYLOR, and STEWART knowing CI#2 did not have a valid DEA registration number, and that CI#2 had been suspended by TMB from treating chronic-pain patients, they had several discussions with CI#2 about hiring CI#2 at SUNNYSIDE #2:

79. On March 22, 2019, CI#2 called ROSENFELD to the number for SUBJECT DEVICE and said that CI#2 had "good news." CI#2 told ROSENFELD had his new DEA number and would it "be okay" if he sent him a copy of his DEA number. ROSENFELD said that it was okay, but that his concern was having the TMB order taken off their website. CI#2 assured ROSENFELD that his lawyer was taking care of the issue. CI#2 then attempted to have

ROSENFELD give CI#2 more details about how ROSENFELD operated the clinic. ROSENFELD hesitated in talking to CI#2 about the details, and said that he wanted CI#2 to remedy his issue with the TMB first.

80. On April 2, 2019, CI#2 called ROSENFELD at the number for SUBECT DEVICE and told him that he got a letter from his attorney showing that his DEA License was not suspended. He also said, "I got my letter from TMB that their updating the website." CI#2 added that he spoke with TAYLOR and was "excited to be working with Dr. Kobza." ROSENFELD told CI#2 to email him the letter from TMB and to make sure TMB's website was updated and then, "We are good." CI#2 then again tried to speak with ROSENFELD about the details of how ROSENFELD prescribed at the clinic. CI#2 told ROSENFELD he spoke to TAYLOR about e-prescribing and asked ROSENFELD to explain how it worked. ROSENFELD told him that after he received confirmation about CI#2's license, that CI#2 would "sit down with Alantha [STEWART] and she'll teach you all about that." This corroborates that ROSENFELD relied on STEWART to control the e-prescribing process so that she could e-prescribe controlled substances while ROSENFELD was usually out of the state.

A. Electronic prescribing

81. Additionally, data obtained from ROSENFELD's electronic prescription provider Surescripts, shows that beginning in or around August 2018, most of ROSENFELD's prescriptions were electronic prescriptions. I know from my training and experience doctors who e-prescribe, often do so from applications on their cellular phones or from a computer. As described above, TAYLOR told CI#2 during a conversation recorded by CI#2, that STEWART e-prescribed controlled substance prescriptions from her cellular phone on ROSENFELD's behalf.

82. On March 22, 2019, CI#2 recorded a meeting with TAYLOR, STEWART and FISHER at SUNNYSIDE #1. CI#2 inquired about how SUNNYSIDE prescribed electronically. TAYLOR responded that the process was easy and that CI#2 would be sent a “hard token” that would be set up on CI#2’s phone, or a key card, to make sure CI#2 is “pushing” the e-prescriptions through. STEWART also spoke with CI#2 about delegating responsibilities to nurse practitioners. TAYLOR told CI#2 that CI#2 would hire a nurse and “you make money through her...she can e-scribe for you.” Given that TAYLOR told CI#2 that they would enable CI#2 to e-prescribe on his phone, and that most of ROSENFELD’s prescriptions were electronically prescribed, it is highly likely that ROSENFELD will have information and applications related to e-prescribing for SUNNYSIDE on SUBJECT DEVICE.

83. Based upon these facts, there is probable cause to believe the SUBJECT DEVICE contains evidence of the crimes discussed above. Accordingly, this affidavit seeks to search and seize SUBJECT DEVICE.

**PROBABLE CAUSE THAT EVIDENCE OF CRIMES IS ON SUBJECT DEVICE
BASED UPON TRAINING AND EXPERIENCE**

84. Based on my training and experience, as outlined above; the facts and circumstances of this investigation; and consultations with experienced narcotics investigators in the DEA and other agencies with extensive knowledge of pharmaceuticals regarding the methods and practices of individuals trafficking in or diverting pharmaceutical controlled substances, I know that persons involved in drug diversion and trafficking, including medical professionals, often maintain and retain on their cellular phones the following:

- a. Records⁷ and information relating to bank accounts, certificates of deposit, stocks, mutual funds, and safe deposit boxes that often contain proceeds of illegal activities;

⁷ The term “records,” used throughout this Section, includes all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including computers and any other electrical, electronic, or magnetic form, such as any information on an electronic or magnetic storage device, including floppy diskettes,

b. Proceeds and records of drug sales and transactions; books, account ledgers, records, receipts, notes, journals, ledgers and other documents relating to financial transactions; and records, and information relating to obtaining, transferring, and spending proceeds of drug diversion and trafficking activities;

c. Records that establish control of various premises, including residences and business premises, including utility bills, cancelled checks, envelopes, deeds, leases, titles, and vehicle registrations;

d. Records and correspondence relating to the order of medical equipment and supplies, and business or professional contracts and agreements;

e. Records containing or relating to names, addresses, phone numbers, email addresses, and personal information of coconspirators, associates, subordinates, employees, and others who join, aid, and abet drug diversion and trafficking in address books, electronic organizers, cellular phones and smart phones, diaries, planners, notebooks, and other physical and electronic storage locations;

f. Patient files and records of office visits, progress notes, prescriptions, urine drug testing, referrals and other patient information. I know under Texas law and by regulation, as described further above, physicians are required to keep records of controlled substance prescriptions they write and dispense. In my training and experience, I know that physicians keep these types of patient records on their cellular phones, and in other electronic formats. I also know based on my training and experience that physicians and clinic owners and managers often transport patient records and documents—both in paper and electronic format on laptops and other electronic storage devices—in their vehicles to other locations, including their residences, to review and update these records.

85. I also know through training and experience, that persons involved in drug diversion and trafficking frequently:

a. Use land line telephones and cellular telephones to conduct business. These persons often attempt to obtain these communication devices through the use of fraudulent or fictitious names, or through the use of nominee subscribers. I further know that evidence of these transactions and the identities of coconspirators and others involved in drug diversion and trafficking can be obtained from telephone and cellular telephone bills and statements; as well as from the telephones, cellular telephones, and associated caller identification devices, voicemail, and answering machines. These bills, business notes, letters and correspondence relating to their business statements, as well as the communications devices, are often stored and maintained in residences and other areas under the dominion and control of those involved in narcotics trafficking;

hard disks, ZIP disks, CD-ROM's, optical discs, thumb drives, backup tapes, printer buffers, smart cards, memory calculators, computer tablets, smart phones, computers, as well as readouts or printouts from any magnetic storage device, any handmade form, any mechanical form, and any photographic form;

b. Attempt to invest their illegal proceeds into legitimate businesses as a means of laundering their drug profits. These organizations often attempt to acquire interest or control of businesses that conduct a large portion of their business in the form of cash and that makes the commingling of drug proceeds with legitimate income an easier task. The acquisition of these legitimate business interests with drug proceeds often creates documentary evidence in the form of bank records, corporation records, financial statements, loan agreements, partnership agreements, and other evidence that is frequently stored or maintained in areas under the dominion and control of the heads of the criminal organization.

c. Communicate about their crimes with coconspirators and others using their mobile phones. Persons involved in drug trafficking often keep their mobile phones on their person or in their residence.

VII. Computers, Electronic Storage, and Forensic Analysis

86. As described above and in ATTACHMENTS B this application seeks permission to search for records that might be found on SUBJECT DEVICE. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

87. I submit that if SUBJECT DEVICE is found on ROSENFELD, there is probable cause to believe records will be stored on the SUBJECT DEVICE, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

88. As further described in ATTACHMENT B, this application seeks permission to locate not only files on SUBJECT DEVICE that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the SUBJECT DEVICE was used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on SUBJECT DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether

the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

89. In most cases, a thorough search of a premises for information that might be stored on storage media, such as cellular phones, often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the

premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a cellular phone has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers, including cellular phones which are essentially mini-computers, can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

90. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

91. The warrants I am applying for would permit law enforcement to seize electronic evidence, including mobile phones, and would compel certain individuals to unlock a device subject to seizure pursuant to this warrant using the device's biometric features. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face. Similarly, Apple's iPhone X (and similar models) has a similar feature that it calls Face ID.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

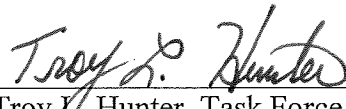
92. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned

biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of ROSENFELD, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

93. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media, including SUBJECT DEVICE, that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

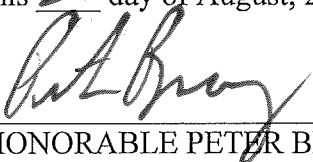
CONCLUSION

94. Based upon the foregoing, probable cause exists to believe that SUBJECT DEVICE contains evidence of violations of Title 21, United States Code, Sections 841(a)(1), unlawful distribution of controlled substances; 846 conspiracy to unlawfully distribute controlled substances; and 856 (a)(2) maintaining a drug-involved premises.



Troy L. Hunter, Task Force Officer
Drug Enforcement Administration

Subscribed to and sworn before me
this 27 day of August, 2019.



HONORABLE PETER BRAY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is ROSENFELD's cell phone with the number 941-456-3635 ("SUBJECT DEVICE"). The warrant requested authorizes federal agents to take possession of the SUBJECT DEVICE from ROSENFELD for imaging—including, if necessary, offsite imaging—wherever it/they may be found in ROSENFELD's custody.

This warrant authorizes the forensic examination of the SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records and information on the SUBJECT DEVICE described in Attachment A that constitute fruits, evidence, and instrumentalities of violations of Title 21 United States Code, Sections 841(a)(1) (unlawful distribution of controlled substances); 846 (conspiracy to unlawfully distribute controlled substances); and 856 (a)(1) (maintaining a drug-involved premises), including but not limited to:

1. Content of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, social media account activity (including browser history, web page logs, and search terms entered by the user), photos, WhatsApp content and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above;
2. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Evidence of the times the devices were used;
4. Passwords, encryption keys, and other access devices that may be necessary to access the devices;
5. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violation described above.

ADDENDUM TO ATTACHMENT B

With respect to law enforcement's review of any MOBILE DEVICE, law enforcement (i.e., the federal agents and prosecutors working on this investigation and prosecution), along with other government officials and contractors whom law enforcement deems necessary to assist in the review of the MOBILE DEVICE (collectively, the "Review Team") are hereby authorized to review, in the first instance, the MOBILE DEVICE and the information and materials contained in them, as set forth in this Attachment B.

If law enforcement determines that all, some, or a portion of the information or materials on the Devices contain or may contain information or material subject to a claim of attorney-client privilege or work-product protection (the "Potentially Privileged Materials"), the Review Team is hereby ordered to: (1) immediately cease its review of the specific Potentially Privileged Materials at issue; (2) segregate the specific Potentially Privileged Materials at issue; and (3) take appropriate steps to safeguard the specific Potentially Privileged Materials at issue.

Nothing in this addendum shall be construed to require law enforcement to cease or suspend the Review Team's review of the MOBILE DEVICE upon discovery of the existence of Potentially Privileged Materials on one or more of the MOBILE DEVICE.

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

In the Matter of the Application by the	§	
United States of America for a Search	§	
Warrant of:	§	Case No.
	§	
ROSENFELD's cell phone with the number	§	UNDER SEAL
941-456-3635	§	
("SUBJECT DEVICE")	§	

UNITED STATES' MOTION TO SEAL SEARCH WARRANT DOCUMENTS

TO THE HONORABLE COURT,

The government files this Motion to Seal the Search Warrant Documents in the above-referenced matter.

The government requests that the Application for a Search Warrant, the Affidavit in support of the Application for the Search Warrant and the Attachments thereto, the Search and Seizure Warrant, the Motion to Seal, and the Order to Seal (collectively, the "Search Warrant Documents"), be sealed. The sealing of these documents is necessary to protect the integrity of the ongoing investigation and to prevent destruction and tampering of evidence that is necessary to complete the investigation. Premature disclosure of these documents could have a significant and negative impact on the ability to continue the investigation and severely jeopardize the effectiveness of the investigation.

Therefore, the government respectfully requests the Court to seal the Search Warrant Documents and that no person shall have access to these documents except the Clerk of the Court or the Clerk's designated deputies, attorneys for the United States, authorized representative and agents of agencies involved in the investigation, and those otherwise acting pursuant to the Court's orders.

Respectfully submitted,

RYAN PATRICK
United States Attorney

By: 

Jason Knutson
Trial Attorney
United States Department of Justice
Fraud Section, Criminal Division
1000 Louisiana Street, Suite 2300
Houston, Texas 77002
Jason.Knutson@usdoj.gov
(713) 567-9428

Date: August 21, 2019

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

In the Matter of the Application by the	§	
United States of America for a Search	§	
Warrant of:	§	Case No.
	§	
ROSENFELD's cell phone with the number	§	UNDER SEAL
941-456-3635	§	
("SUBJECT DEVICE")	§	

ORDER TO SEAL SEARCH WARRANT DOCUMENTS

The government's Motion to Seal the Search Warrant Documents is GRANTED on
August 27, 2019. *for 180 days*

It is ORDERED that *for 180 days* no person shall have access to the Application for a Search Warrant, the Affidavit in support of the Application for the Search Warrant and the Attachments thereto, the Search and Seizure Warrant, the Motion to Seal, and this Order to Seal except the Clerk of the Court or the Clerk's designated deputies, attorneys for the United States, authorized representative and agents of agencies involved in the investigation, and those otherwise acting pursuant to the Court's orders.



Hon. Peter Bray
United States Magistrate Judge